h/c

Sum of 4 square, pp 212 —

AN

ELEMENTARY INVESTIGATION

OF THE

THEORY OF NUMBERS.

AN

1/2 mor Red

ELEMENTARY INVESTIGATION

OF THE

THEORY OF NUMBERS,

WITH ITS APPLICATION TO

THE INDETERMINATE AND DIOPHANTINE ANALYSIS,

THE ANALYTICAL AND GEOMETRICAL DIVISION OF THE CIRCLE,

AND SEVERAL OTHER

CURIOUS ALGEBRAICAL AND ARITHMETICAL PROBLEMS.

BY PETER BARLOW,

OF THE ROYAL MILITARY ACADEMY.

LONDON:

PRINTED FOR J. JOHNSON AND CO.,

ST. PAUL'S CHURCH-YARD.

1811.

Gift of J. Wangenheim
to Math. Dept.

Printed by C. Wood,
Poppin's Court, Fleet Street, London.

PREFACE.

THE Theory of Numbers is a subject which has engaged the attention and exercised the talents of many celebrated mathematicians, both ancient and modern; under the first of which classes, may be reckoned Pythagoras and Aristotle, the former of whom is said to have invented our present multiplication table, or the *Abacus Pythagoricus* of the ancients; though what is alluded to under this designation was probably a much more extensive table than that now in common use: Pythagoras also attributed to numbers certain mystical properties, and seems first to have conceived the idea of what are now termed magic squares. Aristotle, amongst other numerical speculations, noticed the uniformity in almost all nations of dividing numbers into periods of tens, and attempted an explanation of the cause of this singular coincidence upon philosophical principles.

But the earliest regular system of numbers is that given by Euclid in the 7th, 8th, 9th, and

10th books of his Elements, which, notwithstanding the embarrassing notation of the Greeks, and the inadequacy of geometry to the investigation of numerical propositions, is still very interesting, and displays, like all the other parts of the same celebrated work, that depth of thought and accuracy of demonstration for which its author is so eminently distinguished.

Archimedes likewise paid particular attention to the powers and properties of numbers, as may be seen by consulting his tract entitled "Arenarius," in which some modern writers have thought they could perceive inculcated the principles of our present system of logarithms; but all that can be allowed on this head is, that the method by which he performed his multiplications and divisions bears a considerable analogy to that which we now commonly employ in the multiplication and division of powers; that is, by the addition and subtraction of their indices.

Before the invention of analysis, however, no very extensive progress could be made in a subject, which required so much generality of investigation; and, accordingly, we find but little was effected in it till the time of Diophantus, whose treatise of algebra contains many interesting problems in the more

abstruse parts of this science. But here, also, its author had to encounter the difficulties of a complicated notation, and a very deficient analysis, when compared with that of the present period; and, therefore, it cannot be expected that his work should contain a complete investigation of the theory of numbers.

After Diophantus, the subject remained unnoticed, or at least unimproved, till Bachet, a French analyst of considerable reputation, undertook the translation of the abovementioned work into Latin, retaining also the Greek text, which was published by him in 1621, interspersed with many marginal notes of his own, and which may be considered as containing the first germ of our present theory. These were afterwards considerably extended by the celebrated Fermat, in his edition of the same work, published, after his death, in 1670, where we find many of the most elegant theorems in this branch of analysis; but they are generally left without demonstration, an omission which he accounted for by stating, in one of his notes, page 180, that he was himself preparing a treatise on the theory of numbers, which would contain many new and interesting numerical propositions; but, unfortunately, this work never appeared, and most of his

theorems remained without demonstration for a considerable time.

At length, the subject was again revived by Euler, Waring, and Lagrange, three of the most eminent analysts of modern times. The former, besides what is contained in the second volume of his "Elements of Algebra," and his "Analysis Infinitorum," has several papers in the Petersburg Acts, in which are given the demonstrations of many of Fermat's theorems. What has been done by Waring on this subject is comprised in chap. v. of his "Meditationes Algebraicæ;" and Lagrange, who has greatly extended the theory of numbers, by the invention of many new propositions, has several interesting papers on this head, in the Memoirs of Berlin, besides what are contained in his additions to Euler's Algebra.

It is, however, but lately that this branch of analysis has been reduced into a regular system, a task that was first performed by Legendre, in his "Essai sur la Théorie des Nombres;" and nearly at the same time Gauss published his "Disquisitiones Arithmeticæ:" these two works eminently display the talents of their respective authors, and contain a complete development of this interesting theory. The latter, in particular, has opened

a new field of inquiry, by the application of the properties of numbers to the solution of binomial equations, of the form

$$x^n - 1 = 0,$$

on the solution of which depends the division of the circle into n equal parts, as was before known from the Cotesian theorem. This solution he has accomplished in several partial cases, whence the division of the circle into a prime number of equal parts is performed, by the solution of equations of inferior dimensions; and when the prime number is of the form $2^n + 1$, the same may be done geometrically, a problem that was far from being supposed possible before the publication of the abovementioned performance.

From the foregoing historical sketch, it appears that the writers on this subject are far from being numerous; but the well established celebrity of those, who have investigated its principles, would be of itself sufficient to stamp it with a degree of importance, and to render it worthy of attention. Few persons, it is conceived, will be disposed to consider that a barren subject, which has so much engaged the attention of the above named celebrated writers; in fact, there is no branch of analysis that furnishes a greater variety of interesting truths than the theory

of numbers, and it is therefore singular that it should have been so little attended to by English mathematicians. With the exception of what is contained in vol. ii. of Euler's Algebra, and the notes added to the second English edition of that work, there is nothing on this subject to be found in our language.

This circumstance, it is conceived, will be deemed a sufficient apology for the appearance of the present volume; in which, if I have, in certain theorems, availed myself of what others have done on the same subject, yet it is presumed, that it will be found to possess a sufficient degree of novelty, both in matter and arrangement, to exempt me from the imputation of being a *mere copyist*.

With the exception of a few theorems, what is contained in the first six chapters may be considered as new: in the latter of which will be found a demonstration of Fermat's general theorem, on the impossibility of the indeterminate equation

$$x^n \pm y^n = z^n,$$

for every value of n greater than 2; the leading principle of which I first demonstrated in the Appendix to Euler's Algebra, and afterwards completed in vol. xxvii. of the Philosophical Journal. I also consider as original what is contained in chapter x., with the exception

of that part relating to the arithmetic of the Greeks, for which I have been indebted to the Essay of Delambre, subjoined to the French translation of the works of Archimedes. The methods of solving indeterminate equations of the first degree, and of ascertaining, *a priori*, the number of possible solutions, have likewise some claim to novelty. In the other parts of the work, there will also be found several new theorems, and many former ones differently demonstrated, where simplicity and perspicuity could be attained by such alteration: this is particularly the case in the last chapter relating to Gauss's celebrated theorem on the division of the circle. Perspicuity has, indeed, been one of my principal objects; for this treatise being intended for the instruction and amusement of those who may not possess a very extensive knowledge of analysis, it became necessary to make it as clear and intelligible as possible: but how far I may have succeeded in my design, or what merit may be otherwise due to the performance in general, must be left to the decision of the public.

It only remains now for me to mention a circumstance, that may probably be thought to stand in need of some explanation: it will be perceived that I have introduced two new

symbols, the necessity for which, however, will, I trust, appear upon a slight inspection of the work itself: the words *of the form of* recur very often, and the repetition of them would have been tedious and irksome to the reader, for which reason the double f (ff) is introduced instead of them, but, for the sake of uniformity, it is placed lengthwise thus, ⫩; this, therefore, can scarcely be considered as an innovation of a very important rule laid down by modern analysts, "Not to multiply without necessity the number of mathematical symbols." And the same apology may be made for the introduction of the other sign, for the words *divisible by*. These characters were adopted on the suggestion of Mr. Bonnycastle, Professor of Mathematics in the Royal Military Academy, to whose judgment and experience I have been greatly indebted for many important remarks relating to the present performance, and on various other occasions.

PETER BARLOW.

Royal Military Academy, Woolwich,
October 1, 1811.

CONTENTS.

PART I.

CHAP. I. PAGE

On the Sums, Differences, and Products of Numbers in General 1

CHAP. II.

On Divisors, and the Theory of Perfect, Amicable, and Polygonal Numbers 32

CHAP. III.

On the Lineal Forms of Prime Numbers, and their most simple Properties 52

CHAP. IV.

On the possible and impossible Forms of Square Numbers, and their Application to Numerical Propositions 79

CHAP. V.

On the possible and impossible Forms of Cubes, and Higher Powers 123

CHAP. VI.

On the Properties of Powers in General 153

CHAP. VII.

On the Products and Transformations of certain Algebraical Formulæ 176

CHAP. VIII.

On the Quadratic Divisors of certain Algebraical Formulæ 186

CHAP. IX.

On the Quadratic Forms of Prime Numbers, with Rules for determining them in certain Cases . . 200

CHAP. X.

PAGE.
On the different Scales of Notation, and their Application to the Solution of Arithmetical Problems . 220
Notation of the Greeks 245
Miscellaneous Propositions 257

PART II.

CHAP. I.

Continued Fractions, and their Application to various Problems 261

CHAP. II.

On the Solution of Indeterminate Equations of the First Degree 317

CHAP. III.

On the Solution of Indeterminate Equations of the Second Degree 345

CHAP. IV.

On the Solution of Indeterminate Equations of the Third Degree, and those of Higher Dimensions . 396

CHAP. V.

On the Solution of Indeterminate Equations of the Form $x^n - 1 = \text{M}(a)$ 434
Table of Indeterminate Formulæ 452

CHAP. VI.

On the Solution of Diophantine Problems 460
Miscellaneous Problems 476

CHAP. VII.

On the Analytical and Geometrical Division of the Circle 479
Table of Prime Numbers to 4000 506
Table containing the least Values of p and q in the Equation $p^2 - \text{N}q^2 = 1$, *for every Value of* N, *from* 2 *to* 102 507

ERRATA.

Page 20, line 2, *for* "factor," *read* fraction.

24, l. 2 from bottom, *for* "cor. 4," *read* cor. 2.

25, l. 10, *for* "of," *read* as.

35, l. 5, *for* "$z=4$," *read* $z=5$.

35, l. 9, *for* "$2 . 3^2 . 4^4 = 4608$," *read* $2 . 3^2 . 5^4 = 11250$.

37, l. 19, *for* "$\frac{b^{m+1}-1}{a-1}$," *read* $\frac{b^{n+1}-1}{b-1}$.

40, l. 7, add the sign $=$.

54, l. 22, *for* "10000," *read* 4000.

61, l. 8, 9, 10, 11, *for* "If $n=1$," &c., *read* If $a=1$, &c.

75, l. 5, place a comma between a and ± 1.

85, l. 9, *for* "to the squares," *read* as the squares.

89, l. 18, *for* "$\frac{x}{y}$," *read* $\frac{x}{z}$.

90, l. 5, *for* "is not a complete *nth* power," *read* is a complete *nth* power.

90, l. 8, *for* "$2t^2$," *read* $(3p+2)t^2$.

92, l. 19 and 20, *for* "$\doteqdot qu^2$," *read* $\doteqdot 5qu^2$.

95, l. 2, *for* "$7n'-6$," *read* $7n'+6$.

118, l. 3 from bottom, *for* "$2r^2$," *read* $2s^2$.

126, l. 11, *for* "of the same," *read* of the same form.

158, l. 2, *for* "x^n-y^n," *read* x^n+y^n.

178, l. 2 from bottom, *for* "art. 89," *read* art. 91.

179, l. 23, *for* "annunciation," *read* enunciation.

185, l. 21, *for* "x^2+axy," *read* x^2+axx.

185, l. 24, *for* "$-b^2$," *read* $+b^2$.

187, l. 1 of prop. 1, *read* If in the, &c.

192, l. 15, *for* "$pr-y^2$," *read* $pr-q^2$.

260, l. 9 from bottom, *for* "$(n-2)$," *read* $(n-2)^n$

284, l. 8, *for* "u," *read* u'.

Explanation of the new Characters.

$\div$ To be read "divisible by."

$\doteqdot$ To be read "of the form of."

DEFINITIONS.

1. An *Unit*, or *Unity*, is the representation of any thing considered individually, without regard to the parts of which it is composed.

2. An *Integer*, or *Integral Number*, is an unit, or an assemblage of units.

3. A *Fraction*, is any part, or parts, of an unit.

4. *Factors*, are those numbers from the multiplication of which another number is produced.

5. A *Product*, is that number, which is produced by the multiplication of two, or more, factors.

6. A *Multiple* of a number, is the product of that number by some integral factor.

7. An *Even Number*, is that, which can be divided, or separated into two equal integral parts.

8. An *Odd Number*, is that, which cannot be divided into two equal integral parts; being greater or less than some even number by unity.

9. A *Composite Number*, is any number that is produced, by the multiplication of two, or more, factors; or, it is a number which may be divided into two, or more, equal integral parts, each greater than unity.

10. A *Prime Number*, is that which cannot be produced by the multiplication of any integral factors; or it is a number, that cannot be divided into any equal integral parts, greater than unity.

11. *Commensurable Numbers,* are such as have each the same common divisor; or that may be each exactly divided into the same number of equal integral parts.

12. *Incommensurable Numbers,* or *Numbers prime to each other,* are such as have no common divisor.

13. A *Square,* or *2d Power,* is the product of two equal factors.

14. A *Cube,* or *3d Power,* is the product of three equal factors.

15. The *nth Power* of a number, is the product of n equal factors, n representing any integral number whatever.

16. The *Exponent,* or *Index of a Power,* is that number by which the power is expressed: thus, a^n represents a raised to the *nth* power, where n is said to be the Exponent, or Index of the Power.

17. The *Root of a Power,* is that factor from the continued multiplication of which, a certain number of times into itself, the power is produced.

18. A *Perfect Number* is that, which is equal to the sum of all its divisors, or aliquot parts: thus, $6=\frac{6}{2}+\frac{6}{3}+\frac{6}{6}$, and is, therefore, a perfect number.

19. *Amicable Numbers,* are those pairs of integers, each of which is equal to all the aliquot parts of the other: thus, 284 and 220 are a pair of amicable numbers, for

$$\frac{284}{2}+\frac{284}{4}+\frac{284}{71}+\frac{284}{142}+\frac{284}{284}=220, \text{ and}$$

$$\frac{220}{2}+\frac{220}{4}+\frac{220}{5}+\frac{220}{10}+\frac{220}{11}+\frac{220}{22}+\frac{220}{20}+\frac{220}{44}+$$
$$\frac{220}{55}+\frac{220}{110}+\frac{220}{220}=284.$$

20. *Figurate Numbers*, are all those, that fall under the general expression

$$\frac{n.(n+1)(n+2)(n+3)\ \&c.\ n+m}{1\ .\ 2\ .\ 3\ .\ 4\ \&c.\ m+1};$$

and they are said to be of the 1st, 2d, 3d, &c. order, according as $m=1, 2, 3, 4,$ &c.: thus,

								General term.
Nat. series,	1	2	3	4	5	6,	&c.	n
1st ord.	1	3	6	10	15	21,	&c.	$\frac{n.\overline{n+1}}{1.\ 2}$
2d ord.	1	4	10	20	35	56,	&c.	$\frac{n.\overline{n+1}.\overline{n+2}}{1.\ 2.\ 3}$
3d ord.	1	5	15	35	70	126,	&c.	$\frac{n.\overline{n+1}.\overline{n+2}.\overline{n+3}}{1\ .\ 2\ .\ 3\ .\ 4.}$

21. *Polygonal Numbers*, are the sums of different and independent arithmetical series, and are termed *Lineal* or *Natural, Triangular, Quadrangular* or *Square, Pentagonal, Hexagonal,* &c. *Numbers*, according to the series from which they are generated.

22. *Lineal*, or *Natural Numbers*, are formed from the sum of a series of units; thus,

Units, ...	1	1	1	1	1	1	1, &c.
Natural numbers,	1	2	3	4	5	6	7, &c.

23. *Triangular Numbers*, are the successive sums of an arithmetical series, beginning with unity, the common difference of which is 1; thus,

Arith. series,	1	2	3	4	5	6	7, &c.
Triangular numbers,	1	3	6	10	15	21	28, &c.

24. *Quadrangular*, or *Square Numbers*, are the sums of an arithmetical series, beginning with unity, the common difference of which is 2; thus,

Arith. series,	1	3	5	7	9	11, &c.
Quadrang. or square numb.	1	4	9	16	25	36, &c.

25. *Pentagonal Numbers*, are the sums of an arithmetical series, beginning with unity, the common difference of which is 3; thus,

Arith. series,	1	4	7	10	13	16, &c.
Pentagonal numbers,	1	5	12	22	35	51, &c.

26. And universally, the *m-gonal Series of Numbers*, is formed from the successive sums of an arithmetical progression, beginning with unity, the common difference of which is $m-2$.

27. The *Forms of Numbers*, or *Formulæ*, are certain algebraical expressions, under which those numbers are contained. Thus, 17 is of the form $4n+1$, that is, when divided by 4, the remainder is 1; and, for the same reason, 19 is of the form $4n+3$, or $4n-1$; and this is expressed by the character $\doteqdot$: thus $17 \doteqdot 4n+1$, $19 \doteqdot 4n-1$.

28. A *Modulus*, is that number by which the forms of numbers are compared, thus, the forms $4n \pm 1$, are compared by modulus 4, and $6n \pm 1$, by modulus 6.

29. *Numbers of the same Form*, are all those that are contained under the same algebraical ex-

pression, by changing the value of the indeterminate letter, or letters, that enter therein. Thus, 19 and 27 are of the same form, with respect to modulus 4; being each expressed by the same formula, $4n-1$.

30. A *Function of a Quantity*, is any algebraical expression, into which that quantity enters; and it is said to be rational, irrational, or integral, according as the expression is of either of those kinds.

AXIOMS.

1. Every Even Number is of the form $2n$.

2. Every Odd Number is of the form $2n \pm 1$.

3. The Sum, Difference, and Product of any number of integer numbers, are integers.

4. A number cannot be a divisor of another number less than itself.

5. Any number (A) taken once, or one time, is equal to unity, or 1, taken A times. Or, the product $1 \times A = A \times 1$.

AN

ELEMENTARY INVESTIGATION,

&c. &c.

CHAP. I.

On the Sums, Differences, and Products of Numbers in general.

PROPOSITION I.

1. The sum, or difference, of any two even numbers, is an even number.

For all even numbers are of the form $2n$ (ax. 1), and, therefore, the sums and differences of even numbers will be represented by

$$2n \pm 2n' = 2(n \pm n') = 2n'';$$

which is evidently an even number, being of the form $2n$. — Q. E. D.

Cor. The sum of any number of even numbers, is an even number.

PROP. II.

2. The sum, or difference, of two odd numbers, is even; but the sum of three odd numbers, is odd.

For all odd numbers are of the form $2n \pm 1$

(ax. 2.); and, therefore, the sum, or difference, of two odd numbers, will be represented by

$$(2n \pm 1) \pm (2n' \pm 1) = 2(n \pm n' \pm 1) \doteq 2n'',$$

which is evidently an even number, being of the form $2n$.

But the sum of three odd numbers will be expressed by

$$(2n \pm 1) + (2n' \pm 1) + (2n'' \pm 1) =$$
$$2(n + n' + n'' + 1) \pm 1 \doteq 2n''' \pm 1,$$

and is, therefore, an odd number. — Q. E. D.

Cor. 1. The sum of any even number of odd numbers is even; but the sum of any odd number of odd numbers is odd.

Cor. 2. The sum or difference of an even and an odd number is an odd number, for

$$2n \mp (2n' \pm 1) = 2(n \mp n') \pm 1 \doteq 2n'' \pm 1,$$

which is, therefore, an odd number.

PROP. III.

3. The product of an even and an odd number, or of two even numbers, is even. For

$$2n \times (2n' \pm 1) = 2(2nn' \pm n) \doteq 2n'', \text{ and}$$
$$2n \times 2n' = 2(2nn') \doteq 2n'';$$

which are both even forms. — Q. E. D.

Cor. 1. If an even number be divisible by an odd number, the quotient is an even number.

Cor. 2. The product of any number of factors is even, if any one of them be even.

Cor. 3. An odd number cannot be divided by an even number. For if

$$\frac{2n \pm 1}{2n'} = m, \text{ any integer number, then}$$

$$2n' \times m = 2n \pm 1;$$

that is, an even number equal to an odd number, which is absurd; therefore, an odd number cannot be divided by an even number.

Cor. 4. Any power of an even number is even; and, conversely, the root of any complete power is an even number, if the power be so.

PROP. IV.

4. The product of any two odd numbers is an odd number. For

$$(2n \pm 1) \times (2n' \pm 1) = 4nn' \pm 2n \pm 2n' \pm 1 =$$
$$2(2nn' \pm n \pm n') \pm 1 = 2n'' \pm 1,$$

which is evidently an odd number, being of the form $2n \pm 1$. — Q. E. D.

Cor. 1. If an odd number be divisible by any number, the quotient is an odd number.

Cor. 2. The product of any number of odd numbers is odd.

Cor. 3. Every power of an odd number is odd; and, conversely, the root of any complete power is an odd number, if the power be so.

Cor. 4. Since every power of an even number is even (cor. 4, prop. iii.), and every power of an odd number is odd, by the foregoing corollary; therefore, the sum, or difference, of any power and its root, is an even number; that is, if a be any number, and n the exponent of any integral power, then will $a^n \pm a$ be an even number.

PROP. V.

5. If an odd number divides an even number, it will also divide the half of it.

For if an even number be divided by an odd number, the quotient is even (cor. 1. prop. iii.); we have, therefore,

$$\frac{2n}{2n' \pm 1} = 2n'', \text{ and, consequently,}$$

$$\frac{n}{2n' \pm 1} = n'', \text{ an integer:}$$

therefore n, which is half the even number $2n$, is divisible by $(2n \pm 1)$, if $2n$ be so. — Q. E. D.

Cor. If an even number be divisible by an odd number, it will also be divisible by double that number.

PROP. VI.

6. If a number, p, divide each of two other numbers, a and b, it will also divide the sum and difference of those numbers; or the sum and difference of any multiples of them. For let

$$\frac{a}{p} = q, \text{ and } \frac{b}{p} = q', \text{ then will}$$

$$\frac{a}{p} \pm \frac{b}{p} = \frac{a \pm b}{p} = q \pm q',$$

and since q and q' are each integers by the hypothesis, therefore, $q \pm q'$ is also an integer (ax. 3); and, consequently, $a \pm b$ is divisible by p. Again, if ma, and nb, represent any multiples of a and b; then, since $\frac{a}{p} = q$, and $\frac{b}{p} = q'$, therefore, $\frac{ma}{p} = mq$, and $\frac{na}{p} = nq'$; consequently $\frac{ma}{p} = \frac{nb}{p} = \frac{ma \pm nb}{p} = mq \pm nq'$. And because both q and q', as also m and n, are integers, therefore $mq \pm nq'$ is likewise an

integer (ax. 3), and, consequently, $ma \pm nb$, is divisible by p. — Q. E. D.

Cor. 1. Hence, if a number divides the whole of another number, and a part of it, it will also divide the other part.

Cor. 2. Hence, also, if a number consists of many parts, and each of those parts have a common divisor p; then will the whole number, taken collectively, be divisible by p.

PROP. VII.

7. If a and b be any two numbers prime to each other, then will their sum, $a+b$, be also prime to each of them.

For if $(a+b)$ and a, had any common divisor p, then $(a+b)-a$ and a, would also have the same common divisor (prop. vi.); that is, a and b would have a common measure, which is contrary to the supposition, because they are prime to each other; therefore $(a+b)$ and a, cannot have a common measure. And in the same manner it may be shown, that $(a+b)$ and b, can have no common measure; and, consequently, if a and b be any two numbers prime to each other, their sum $a+b$ is prime to each of them. — Q. E. D.

Cor. 1. In the same manner it may be demonstrated, if a and b be any two numbers prime to each other, that their difference $(a-b)$ is prime to each of them, if $(a-b) > 1$.

Cor. 2. If a number, consisting of two parts, as $(a+b)$, be prime to one of its parts a, it will also be prime to the other part b, if $b > 1$.

Cor. 3. If of two numbers, a and b, one of them

be divisible by a third number p, but the other part not divisible by it, then neither the sum nor difference of those numbers $(a \pm b)$ is divisible by p.

Cor. 4. If a number, consisting of many parts, have all those parts but one divisible by another number p, but the other part not divisible by it, then the whole number, taken collectively, is not divisible by p.

PROP. VIII.

8. If a and b be any two numbers prime to each other, then will their sum and difference, $(a+b)$ and $(a-b)$, be also prime to each other, or they will only have the common measure 2.

For if $(a+b)$, and $(a-b)$, have any common measure, their sum and difference, $2a$ and $2b$, will have the same (prop. VI.); but since a and b are prime to each other, $2a$ and $2b$ can only have the common measure 2; therefore $(a+b)$ and $(a-b)$, can only have the same common measure 2: and, consequently, if one of those quantities, a or b, be even, and the other odd, then $(a+b)$ and $(a-b)$, being both odd, cannot have the common measure 2; therefore, in this case, they are prime to each other. — Q. E. D.

PROP. IX.

9. The product of any two numbers is the same, which ever of the two is the multiplier; or $a \times b = b \times a$.

First, if $a = b$, then it is evident that $ab = ba$; but if these factors are not equal, one of them must be the greatest: let, then, $a > b$, and make $a = b + a'$,

in which a' is necessarily less than a, then

$$ab = bb + a'b, \text{ and}$$
$$ba = bb + ba';$$

if, therefore, ab is different from ba, so also is $a'b$ different from ba', for the equality of the products ab and ba, depends upon the equality of the products $a'b$ and ba'. Now if in this last, $a' = b$, the equality is established, as it is also if $a' = 1$, because, $1 \times b = b \times 1$ (ax. 5).

But if neither $a' = b$ nor $a' = 1$, then one of these factors is the greatest; let then $b > a'$, and make $b = a' + b'$, where $b' < b$, and we have

$$a'b = a'a' + a'b'$$
$$ba' = a'a' + b'a',$$

and the equality of the products $a'b$ and ba' now depends upon the equality of the products $a'b'$ and $b'a'$, and, therefore, the equality of the first products ab and ba, depends also upon the equality of these last; and if in this, $b' = a'$, or $b' = 1$, the equality is established; but if not, by proceeding as above, we may show, that the equality of these products depends upon others still less, and so on.

Now it is evident, that in the products ab, ba; $a'b$, ba'; $a'b'$, $b'a'$, &c., in which we have $a' < a$, $a'' < a'$, $b' < b$, $b'' < b'$, &c.; we must necessarily arrive at a case in which the terms of the product are equal, or in which one of them is equal to unity; and in either case the identity of the original products is established, from what is said above and by ax. 5; and, consequently, the product $ab = ba$. — Q. E. D.

Cor. In a similar manner it may be shown, that the product of any number of factors, $a\ b\ c\ d$, &c., is the same, in whatever order they are multiplied together.

PROP. X.

10. If a and p be any two numbers prime to each other, then may either of these numbers, as a, be expressed by the formula

$$a = np + r,$$

in which r shall be less than p, and also prime to it.

For, first, if $a < p$, we may make $n = 0$, or

$$a = 0 \times p + r, \text{ or } a = r;$$

and, since $a < p$, and $r = a$, therefore $r < p$. But if $a > p$, let a be divided by p, giving a quotient n, and remainder r, which makes $a = np + r$; and since r is the remainder arising from a divisor p, it is evident that we may have $r < p$.

Again, r is also prime to p; for if p and r had a common measure, then $np + r$ and p would have the same common measure (prop. vi.), but $a = np + r$, therefore a and p would have a common measure, which is contrary to the supposition, because a and p are prime to each other; therefore, in the formula, $a = np + r$, n may be so assumed, that $r < p$, and it is necessarily prime to it.—Q. E. D.

Cor. Hence, also, it appears, that a and p being prime to each other as before, we may always make

$$a = np \pm r,$$

so that r shall be less than $\frac{1}{2}p$, and also prime to it.

For, by the foregoing proposition, the formula

$$a = np + r$$

is always possible, so that $r < p$. And if at the same time $r < \frac{1}{2}p$, it agrees with the enunciation of this corollary; but if $r > \frac{1}{2}p$, then $(p - r) = r' < \frac{1}{2}p$; and it is evident that

$$a = np + r = (n+1)p - (p-r) = n'p - r',$$

by making $n + 1 = n'$, and $(p - r) = r'$, in which, as we have seen above, $p - r$, or $r' < \frac{1}{2}p$: therefore, in the formula

$$a = np \pm r,$$

n may always be so assumed, that $r < \frac{1}{2}p$; and that it is prime to it, is evident from what has been observed in the proposition.

Cor. 2. This formula, $a = np \pm r$, is equally true of numbers not prime to each other, except that here p and r are not necessarily prime to each other, and r may also, in this case, become zero, which cannot be in the former.

PROP. XI.

11. If a and p be any two numbers prime to each other, there cannot be another number b, prime to p, that renders the product ab divisible by p. Or if a number, p, be prime to two other numbers, a and b, it will also be prime to their product ab.

First, it is evident, that if there be such a number b, prime to p, it is either the only one, or there are others besides itself; in either of which cases, we may suppose b to be the least of all those numbers that are prime to p, and that renders the product ab divisible by p. Now since b is prime to p, we may make

$$p = nb + b',$$

in which formula, $b' < b$, and also prime to both p and b (prop. x.); also b' cannot be o, because p is prime to b. Again, multiplying both sides of this formula by a, we have

$$ap = nab + ab', \text{ or}$$
$$ap - nab = ab'.$$

And here it is evident, that if the product ab be divisible by p, the first side of the above equation, $ap - nab$, will be so likewise (prop. vi.); and, consequently, the equal quantity ab', will be divisible by p: but $b' < b$, and b is the least of all numbers that renders the product ab divisible by p; whereas we have now found a less, which is absurd. There cannot, therefore, be a number, which is the least of all those, that render the product ab divisible by p; but if there were any such numbers, one of them must necessarily be the least; therefore, there are no such numbers; and, consequently, if p be prime to two other numbers, a and b, it is also prime to their product ab. — Q. E. D.

Cor. 1. If a number p be prime to any number of quantities or factors, a, b, c, d, &c., it is also prime to their product, $abcd$, &c. And if p be prime to any number a, it is prime to every factor of a.

Cor. 2. Hence a product can only be divided by those numbers, or factors, from the multiplication of which it is produced; and, therefore, if ab be divisible by p, it is divisible by every factor of p.

Cor. 3. If in cor. 1 the factors are equal, that is, if $a = b = c = d$, &c., then the continued product, $abcd$, becomes some power of a, as a^n; and, therefore, if p be prime to a, it is prime to every power of a.

Cor. 4. A power of any number, as a^n, can only have the same prime divisors as a.

Cor. 5. If p be a divisor of the product ab, and be prime to one of its factors, as a, it will be a divisor of the other factor b. And if there be any number of factors, a, b, c, d, the product of which $abcd$, be divisible by p, and of which quantities one

of them, as a, be prime to p, then will the product of the other factors bcd, &c., be also divisible by p.

Cor. 6. If a be prime to p, and b less than p, then, whether b be prime or not to p, the product ab is not divisible by p.

Cor. 7. If there be any number of quantities a, b, c, d, &c., and also any number of other quantities, p, q, r, s, &c.; and of which all the former are respectively prime to each of the latter, then will the products of those sets of factors be prime to each other.

Cor. 8. If a product ab, be divisible by p, and one of those factors, as a, be prime to p, then will the quotient be divisible by a. For, by cor. 5, if ab be divisible by p, and a prime to p, then is b divisible by p: let, therefore, $\frac{b}{p} = q$, then will $\frac{ab}{p} = aq$, and, consequently, the quotient aq is divisible by a.

PROP. XII.

12. The coefficient of every term of the expanded binomial $(a \pm b)^n$, is an integer number, when n is an integer.

First, we know from the binomial theorem, that each of those terms is of the form

$$\frac{n \, . \, (n-1)(n-2)(n-3) \; - - - \; (n-r)}{1 \, . \, 2 \, . \, 3 \, . \, 4 \; - - - - \; (r+1)}.$$

Now n must be of one of the forms $2n'$, or $2n'+1$; and, therefore, one of the first two factors is divisible by 2. Again, n must be of one of the forms $3n'$, $3n'+1$, or $3n'+2$; and, therefore, one of the first three factors, in the numerator, must have the form $3n'$; that is, one of those terms is divisible by 3.

Also n must be of one of the forms $4n'$, $4n'+1$, $4n'+2$, or $4n'+3$, and, therefore, one of the first four terms is of the form $4n'$; that is, one of those terms is divisible by 4; and in the same manner it may be shown, that one of the first five terms is divisible by 5, and so on; and, there being as many terms in the numerator as in the denominator, and each term in the denominator being a divisor of some one term in the numerator, it follows, that the whole product of the former terms is a divisor of the whole product of the latter; and, consequently, as the coefficient of each term is of the above form, it is an integer. — Q. E. D.

Cor. 1. If n be a prime number, then each of the coefficients, except the first and last, in the expanded binomial $(a \pm b)^n$, is divisible by n. For n being a prime number, it is prime to every factor in the denominator, these being all less than n, and, consequently, n is prime to the whole product in the denominator; that is, calling the product of all the terms in the numerator, except the first, N; and those in the denominator D; we have $\frac{n\text{N}}{\text{D}} = q$, an integer: but since n is prime to D, the quotient $\frac{n\text{N}}{\text{D}} = q$, is divisible by n (cor. 8, prop. xi.); that is, each of the coefficients, except the first and last, is divisible by n, when n is a prime number. And, therefore, in any case, where the nature of the investigation requires such a substitution, we may put for the coefficients of the expanded binomial $(x+y)^n$, when n is a prime, the series

$$1,\ n,\ na,\ nb,\ \&c.\ nb,\ na,\ n,\ 1,$$

and in which we shall always have a, b, c, &c., integral numbers; but such a substitution cannot be generally made, if n be a composite number.

PROP. XIII.

13. Neither the sum nor the difference of two fractions, which are in their lowest terms, and of which the denominator of the one contains a factor not common with the other, can be equal to an integer number.

Let $\frac{a}{\text{A}}$, and $\frac{b}{\text{B}t}$, be any two fractions in their lowest terms, and of which the denominator of the one, as $\frac{b}{\text{B}t}$, contains a factor t, that is not contained in A; then I say, that

$$\frac{a}{\text{A}} \pm \frac{b}{\text{B}t} = e,$$

an integer, is, in all such cases, impossible. For,

$$\frac{a}{\text{A}} \pm \frac{b}{\text{B}t} = \frac{a\text{B}t \pm \text{A}b}{\text{AB}t};$$

and if this expression can be equal to an integer, the numerator $a\text{B}t \pm \text{A}b$, must be divisible by the denominator $\text{AB}t$; and, consequently, by each of its factors A, B, and t (cor. 2, prop. x.); but it cannot be divisible by t, for if it was, $\pm \text{A}b$ must be divisible by t, because the other part $a\text{B}t$ is divisible by it (cor. 1, prop. vi.): but since $\frac{b}{\text{B}t}$ is in its lowest terms, b is prime to $\text{B}t$, and, therefore, necessarily prime also to t, and A is likewise prime to t by the hypothesis, consequently $\text{A}b$ is not divisible by t

(prop. xi.). Since, then, the numerator $a\text{B}t \pm \text{A}b$ is not divisible by the denominator, the ~~factor~~ f...

$$\frac{a\text{B}t \pm \text{A}b}{\text{AB}t}, \text{ or its equal } \frac{a}{\text{A}} \pm \frac{b}{\text{B}t},$$

cannot be equal to an integer. — Q. E. D.

Cor. 1. The same is also true, if the first fraction $\frac{a}{\text{A}}$, be not in its lowest terms, providing the other fraction $\frac{b}{\text{B}t}$ be in its lowest terms, and the factor t, of this last, not common with A; for we should still have, in this case, t prime both to A and b, and, consequently, also to the product $\text{A}b$, and likewise to the numerator $a\text{B}t \pm \text{A}b$; and, therefore,

$$\frac{a\text{B}t \pm \text{A}b}{\text{AB}t}, \text{ or its equal } \frac{a}{\text{A}} \pm \frac{b}{\text{B}t} = e,$$

an integer, is impossible.

Cor. 2. In the same manner it may be shown, if there be several fractions, as

$$\frac{a}{\text{A}}, \frac{b}{\text{B}t}, \frac{c}{\text{C}}, \frac{d}{\text{D}}, \text{ \&c.},$$

and one of them, as $\frac{b}{\text{B}t}$, be in its lowest terms, and contain a factor t, in its denominator, that is not common to all the other denominators; that these fractions cannot, however they may be combined, be equal to an integer; that is,

$$\frac{a}{\text{A}} \pm \frac{b}{\text{B}t} \pm \frac{c}{\text{C}} \pm \frac{d}{\text{D}} = e,$$

an integer, is impossible, under the specified limitations.

Cor. 3. The sum, or difference, of two fractions, both being in their lowest terms, is also in its lowest terms, if the denominators of the given fractions be prime to each other.

For let $\frac{a}{\text{A}}$, and $\frac{b}{\text{B}}$, be both in their lowest terms; then is their sum, or difference,

$$\frac{a}{\text{A}} \pm \frac{b}{\text{B}} = \frac{a\text{B} \pm b\text{A}}{\text{AB}},$$

also a fraction in its lowest terms: because $a\text{B}$ is prime to A, and $\pm b\text{A}$ prime to B.

Cor. 4. If $\frac{a}{\text{A}}$, and $\frac{b}{\text{B}}$, be two fractions in their lowest terms; then is their product $\frac{ab}{\text{AB}}$ also in its lowest terms, as is evident by cor. 7, prop. xi.

PROP. XIV.

14. Every number p, without exception, may be represented by the formula $a^n b^m c^q$, &c.

For if p be a prime number, then we shall have $b=1$, $c=1$, &c., and $n=1$, which makes $p=a$. And if p be a composite number, and a, b, c, &c., its prime factors, let it be divided by the highest powers of a contained in it, as a^n; and the quotient by the highest powers of b contained in it, as b^m; and the quotient again by the highest powers of c contained in it, as c^q; and so on, as long as division can be made, so shall we have

$$p = a^n b^m c^q, \text{ \&c.} \qquad \text{Q. E. D.}$$

Cor. 1. From the foregoing proposition it ap-

pears, that the least divisor of every number is a prime number.

Cor. 2. It follows, also, from the above proposition, and cor. 2, prop. xi., that any number p being resolved into the form $a^n b^m c^q$, &c., its divisors will be all of the same form, *viz.* $a^r b^s c^t$, &c.; in which form, no one of the exponents r, s, t, &c., can exceed the corresponding exponents n, m, q, &c.; because no number can be divided but by those factors, from the multiplication of which the number is produced (cor. 2, prop. xi.).

Cor. 3. Hence, also, we see how the greatest common divisor of two or more numbers is obtained; for, having resolved them into their factors, as above, the greatest common measure will be the greatest power of those factors that enter into each number: this method is, however, rather theoretical than practical, being by no means so ready in application as the rule generally given for this purpose in books of arithmetic.

Cor. 4. Since every number $p = a^n b^m c^q$, &c., every square number $p^2 = a^{2n} b^{2m} c^{2q}$, &c.; and, therefore, if $p = a^n b^m c^q$, &c., and any one of the exponents n, m, q, &c., is an odd number, that number p is not a square, but may be represented by the form $p = \text{A}^2 abc$, &c.

In the same manner, every cube number $p^3 = a^{3n} b^{3m} c^{3q}$, &c., and, consequently, if any number $p = a^n b^m c^q$, &c., and any one of the exponents n, m, q, &c., be not divisible by 3, that number is not a cube.

Cor. 5. If p be a square number, all the powers

of its factors, a, b, c, &c., are even; for let $p'^2 = p$, and resolve p' into its factors, as $p' = a^m b^n$, &c., then p'^2 or $p = a^{2m} b^{2m}$, &c., that is, the powers of a, b, &c., are all even. And hence again, if p be not a square, those powers will not be all even, but p will, in this case, be of the form $a^{2n} b^{2n} cd$, or $\text{A}^2 cd$, where c and d are prime numbers.

PROP. XV.

15. If a square number be either multiplied or divided by a square, the product, or quotient, is a square; and conversely, if a square number be either multiplied or divided by a number that is not a square, the product, or quotient, is not a square.

For let p^2 be the proposed square, and let p be resolved into its factors, as in the foregoing proposition; *viz.* make $p = a^n b^m c^q$, &c., then $p^2 = a^{2n} b^{2m} c^{2q}$, &c.; and if p'^2 be the proposed square divisor, then (cor. 2, prop. xiv.) p' must contain some one, or more, of the prime factors of p; namely, a, b, c, &c., therefore, resolving p' into its factors, we shall have $p' = a^r b^s c^t$, &c.; and $p'^2 = a^{2r} b^{2s} c^{2t}$, &c.; also

$$\frac{p^2}{p'^2} = \frac{a^{2n} b^{2m} c^{2q}}{a^{2r} b^{2s} c^{2t}} = a^{2(n-r)} \times b^{2(m-s)} \times c^{2(q-t)},$$

which is evidently a square.

And, with respect to the product, it is obvious that $p^2 \times p'^2 = p^2 p'^2$, is a square, its root being pp'.

Again, if the multiplier p' be not a square, then I say, that $p^2 p'$ is not a square, for if $p^2 \times p' = r^2$,

then $\frac{r^2}{p^2}=p'$ would be a square by the foregoing part of the proposition, which is contrary to the supposition; therefore, p^2p' is not a square. Neither is $\frac{p^2}{p'}$ a square; for if $\frac{p^2}{p'}=r^2$, then would $p^2=r^2p'$, or, $p'=\frac{p^2}{r^2}$, but $\frac{p^2}{r^2}$ is a square, therefore p' is a square, which is contrary to the supposition, and, consequently, $\frac{p^2}{p'}$ is not a square. — Q. E. D.

Cor. In the same manner it may be shown, that $p^3 \times p'^3$ and $\frac{p^3}{p'^3}$ are both cubes: but $p^3 \times p'$, and $\frac{p^3}{p'}$ are not cubes, if p' be not a cube. And generally, $p^n \times p'$ and $\frac{p^n}{p'}$ are both *nth* powers, if p' be an *nth* power, but otherwise they are not.

PROP. XVI.

16. If the square of a number, as p^2, can be divided *once*, by some other number, as p', and after that, neither by p', nor by any factor of p', then will p' itself be a complete square.

For let p be resolved into its factors, making

$$p=a^n b^m c^q, \text{ \&c., or } p^2=a^{2n}b^{2m}c^{2q};$$

and since p^2 is divisible by p', p' must contain some one, or more, of the prime factors of p (cor. 2, prop. xiv.); that is, p' must be of the form $a^r b^s$, &c.; and hence

$$\frac{p^2}{p'} = \frac{a^{2n}b^{2m}c^{2q}, \text{ \&c.}}{a^r b^s, \text{ \&c.}} = a^{2n-r}b^{2m-s}c^{2q},$$

which quotient will evidently be still divisible by some one of the factors of p', unless $r = 2n$, and $s = 2m$; and since by the supposition this quotient is not again divisible, either by p' or by any factor of p', therefore it follows, that $p' = a^{2n}b^{2m} = (a^n b^n)^2$; that is, p' is itself a complete square. — Q. E. D.

Cor. In the same manner it may be shown, if p^3 be divisible once by some other number of p', and after that, neither by p' nor by any factor of p', that p' is a complete cube. And generally, if p^n be divisible once by p', and after that, neither by p' nor by any factor of p', then will p' be a complete *nth* power.

PROP. XVII.

17. The product arising from two different prime numbers cannot be a square number.

For let p and q represent any two prime numbers, that are not equal to each other, and, if possible, let also $pq = m^2$; or $\frac{pq}{m} = m$. But a number can only be divided by those prime factors from the multiplication of which it is produced (cor. 2, prop. xi.); therefore, pq being divisible by m, either $m = p$, or $m = q$: let $m = p$, then $\frac{pq}{p} = q$; but $\frac{pq}{m} = m$; therefore also $m = q$, which is absurd, since $m = p$, and p and q are unequal numbers; therefore $pq = m^2$ is impossible, when p and q are two unequal prime numbers. — Q. E. D.

Cor. 1. In the same manner it appears, that the

product of any number of unequal prime numbers can never produce a square.

Cor. 2. By means of this proposition, it may also be shown, that the product of any two numbers prime to each other cannot produce a square, unless each of those numbers be a square.

For every number p, that is not a square, may be represented by the formula $p=\text{A}^2cd$, c and d being prime numbers (cor. 5, prop. xiv.): let, therefore, p and q be two numbers prime to each other, and not both squares, and make

$$p=\text{A}^2cd, \text{ and } q=\text{A}'^2tv;$$

then $pq=\text{A}^2\text{A}'^2cdtv$, one part of which product is a square, and the other part prime numbers, all different from each other, because p is prime to q; and, therefore, this latter part $cdtv$, cannot be a square, by cor. 1, and consequently the product of $\text{A}'^2\text{A}^2\times cdtv$ is not a square (prop. xv.); that is, pq is not a square. The case in which one of the numbers, as p, is a square, needs no demonstration.

Cor. 3. All that has been demonstrated in this proposition and its corollaries, is equally true for cubes, and all higher powers; namely, the product of two numbers p and q, prime to each other, can never produce an *nth* power, unless each of those numbers be complete *nth* powers.

Cor. 4. If the product of two numbers be a square, each of those numbers is a square, or they are each the same multiple of squares: and if the product of the two quantities $mn=ay^2$, a being a prime, then must $m=ast^2$, and $n=st'^2$, or the contrary, $n=ast^2$ and $m=st'^2$; and if

$a=bc$, then must $m=bst^2$, and $n=cst'^2$; or $m=bcst^2$, and $n=st'^2$, or the contrary, as is evident.

Cor. 5. Hence, also, the product of the square roots of two numbers not squares, and prime to each other, cannot produce an integer: for if $\sqrt{p}\times\sqrt{q}$, or $\sqrt{pq}=r$, then $pq=r^2$, which we have seen is impossible when p and q are prime to each other. And the same is also true of any number of quantities, $\sqrt{p}\times\sqrt{q}\times\sqrt{r}$, &c., if p, q, r, &c., be prime to each other, and not all square numbers.

PROP. XVIII.

18. The square root of an integer number, that is not a complete square, can neither be expressed by an integer, nor by a rational fraction.

For let a represent any integer number, that is not a complete square, then it is evident that it can have no integral root, from the definition of square numbers; and it is to be demonstrated, that neither can it have any rational fractional root.

Now, if it be possible, let $\sqrt{a}=\frac{m}{n}$, the fraction $\frac{m}{n}$ being supposed to be in its lowest terms, so that m is prime to n; then $\frac{m^2}{n^2}=a$, and, consequently, m^2 must be divisible by n^2; but since m is prime to n, the product, or square, m^2 is also prime to n^2 (cor. 7, prop. xi.); therefore, m^2 cannot be divisible by n^2, or $\frac{m^2}{n^2}=a$, is impossible, and consequently so is also $\sqrt{a}=\frac{m}{n}$. — Q. E. D.

Cor. 1. In the same manner it may be shown, that the cube root of an integer, that is not a complete cube, can never be represented by any rational fraction; and generally, if a be an integer, and $\sqrt[n]{a}$ cannot be represented by an integer, it is also impossible to represent it by any rational fraction.

Cor. 2. The product of the square root of two numbers prime to each other cannot be expressed by any rational fraction. For if p and q were two numbers prime to each other, and $\sqrt{p} \times \sqrt{q} = \frac{m}{n}$, we should have also $\sqrt{pq} = \frac{m}{n}$, which is impossible by the above proposition, because the product pq is not a square (cor. 2, prop. xvii.).

Cor. 3. In the same manner it may be shown, that the product of the cube roots of two numbers prime to each other, and not both cubes, cannot be represented by any rational fraction; and generally, if p and q be any two integer numbers, prime to each other, then the product $\sqrt[n]{p} \times \sqrt[n]{q}$, cannot become equal to any rational quantity, unless p and q be each complete *nth* powers, and in this case the product is an integer.

Cor. 4. All that has been demonstrated in the above two corollaries, of two quantities prime to each other, is equally true of any number of quantities under the same restrictions.

PROP. XIX.

19. Neither the sum, nor difference, of the square roots of two quantities, prime to each other, can be represented by any rational quantity; nor by the

square root of any rational quantity; unless each of those numbers be a complete square.

For let p and q be any two such numbers, and, if it be possible, let also

$$\sqrt{p} \pm \sqrt{q} = c,$$

c representing any rational quantity, or the square root of any rational quantity; then, by squaring, we have

$$(\sqrt{p} \pm \sqrt{q})^2 = c^2 = p + q \pm 2\sqrt{pq};$$

and since c is either rational, or the square root of a rational quantity, c^2 is in either case rational; and, consequently, also

$$c^2 - p - q = \pm 2\sqrt{pq}, \text{ or}$$

$$\sqrt{pq} = \frac{c^2 - p - q}{\pm 2},$$

is also a rational fraction, which is impossible (cor. 2, prop. xviii.); and, consequently,

$$\sqrt{p} \pm \sqrt{q} = c, \text{ or } = \sqrt{c},$$

is also impossible. — Q. E. D.

Cor. It may likewise be demonstrated, by means of this proposition, p and q, being prime as before, and not both squares, that neither the sum nor difference of their roots can be represented by the sum or difference of the roots of any other two integral quantities whatever, that are prime to p and q; that is,

$$\sqrt{p} \pm \sqrt{q} = \sqrt{r} \pm \sqrt{s}$$

is impossible.

For, by squaring, we have

$$p + q \pm 2\sqrt{pq} = r + s \pm 2\sqrt{rs}, \text{ or}$$

$$\pm \sqrt{pq} \mp \sqrt{rs} = \frac{r + s - p - q}{2}.$$

Now either $\sqrt{rs}$ is rational, or it is not; if it be rational, so also must be

$$\pm \sqrt{pq} = \frac{r+s-p-q}{2} - \sqrt{rs},$$

which it cannot be (cor. 2, prop. xviii.); therefore, $\sqrt{rs}$ cannot be rational.

Again, if $\sqrt{rs}$ be not rational, then we should have

$$\sqrt{pq} \pm \sqrt{rs} = \frac{r+s-p-q}{2},$$

a rational quantity; which is also impossible by the above proposition, because pq and rs are prime to each other, and, consequently,

$$\sqrt{p} \pm \sqrt{q} = \sqrt{r} \pm \sqrt{s}$$

is impossible, under the specified limitations.—Q.E.D.

PROP. XX.

20. If in any equation whatever, higher than the first degree, the coefficient of the first term be unity, and those of the other terms integral numbers, then no one of the roots of such an equation can be equal to a rational fraction.

For let $x^n \pm ax^{n-1} \pm bx^{n-2} \pm$, &c., $\pm r = o$, represent a general form of equation; and, if it be possible, let $x = \frac{p}{q}$, the fraction $\frac{p}{q}$ being supposed already in its lowest terms; then, by substituting $\frac{p}{q}$ for x, the equation becomes

$$\frac{p^n}{q^n} \pm \frac{ap^{n-1}}{q^{n-1}} \pm \frac{bp^{n-2}}{q^{n-2}} \pm \frac{cp^{n-3}}{q^{n-3}} \pm, \text{ \&c., } \pm r = o; \text{ or,}$$

$$\frac{p^n \pm aqp^{n-1} \pm bq^2p^{n-2} \pm cq^3p^{n-3} \pm, \&c.,}{q^n} = \mp r; \text{ or,}$$

$$\frac{p^n \pm q(ap^{n-1} \pm bqp^{n-2} \pm cq^2p^{n-3} \pm, \&c.)}{q^n} = \mp r.$$

Now as this is equal to r, an integer, it follows that the numerator is divisible by q^n; and, therefore, also by q; but since the part

$$q(ap^{n-1} \pm bqp^{n-2} \pm cq^2p^{n-3} \pm, \&c.)$$

is divisible by q, it is evident that p^n must also be divisible by q, if the whole quantity be so (cor. 1, prop. vi.); but this is impossible, because p is prime to q, therefore the numerator is not divisible by q; and, consequently, $x=\frac{p}{q}$ is impossible. — Q. E. D.

CHAP. II.

On Divisors, and the Theory of Perfect, Amicable, and Polygonal Numbers.

PROP. I.

21. Any number N being reduced to the form $N = a^m b^n c^p d^q$, &c., the number of its divisors will be expressed by the formula

$$(m+1)\times(n+1)\times(p+1), \text{ \&c.}$$

For it is evident, that N will be divisible by a, and every power of a, to a^m; that is, by each of the terms

$$1,\ a,\ a^2,\ a^3,\ \text{\&c.},\ a^m.$$

Also by b, and every power of b, to b^n; that is, by every term in the series

$$1,\ b,\ b^2,\ b^3,\ \text{\&c.},\ b^n.$$

And, in the same manner, N is divisible by c, and every power of c, to c^p; by d, and every power of d, to d^q, &c.; and also by every possible combination of the respective terms of the above series; that is, by every term of the continued product,

$$(1+a+a^2+, \text{\&c.}, a^m)\times(1+b+b^2+, \text{\&c.}, b^n)\times$$
$$(1+c+c^2+, \text{\&c.}, c^p)\times(1+d+d^2+, \text{\&c.}, d^q).$$

But the number of terms of this product, since no two of them can be the same, is truly expressed by the formula

$$(m+1)\times(n+1)\times(p+1)\times(q+1), \text{ \&c.};$$

therefore, the number of the divisors of N is also expressed by the same formula. — Q. E. D.

Remark. It will readily be observed, that, in the above formula, N is considered as a divisor of itself.

Ex. 1. Having given the number 360, to find the number of its divisors.

First, $360 = 2^3.3^2.5^1$; therefore, $n=3$, $m=2$, and $p=1$. Hence,

$$(3+1)\times(2+1)\times(1+1)=4\times3\times2=24,$$

the number of its divisors.

Ex. 2. It is required to find how many numbers there are, by which 1000 is divisible.

First, $1000=2^3 . 5^3$; or $m=3$, and $n=3$; therefore, $(3+1)\times(3+1)=4\times4=16$: that is, there are 16 numbers by which 1000 is divisible.

Cor. 1. As the number of divisors of any given number, $N = a^m b^n c^p$, &c., is represented by the formula

$$(m+1)\times(n+1)\times(p+1), \text{ \&c.},$$

it is evident, that the number of ways, in which the given number N may be resolved into two factors, will be represented by

$$\frac{1}{2}\times(m+1)\times(n+1)\times(p+1), \text{ \&c.},$$

because every divisor has its reciprocal factor; and, therefore, the number of ways, in which a number may be resolved into two factors, is equal to half the formula, that expresses the number of its divisors. But if the given number N be a square, then all the exponents, m, n, p, &c., will be even, and, therefore,

$$(m+1)\times(n+1)\times(p+1), \text{ \&c.},$$

will be odd; and the formula, representing the num-

ber of ways that N may be resolved into two factors, will be

$$\frac{(m+1)\times(n+1)\times(p+1), \text{ \&c.}, +1}{2};$$

because, in this case, two of the factors are equal.

Cor. 2. If it be required, in how many ways a number, $N = a^m b^n c^p$, &c., may be resolved into two factors prime to each other, it is evident, that this number no longer depends upon the value of the exponents m, n, p, &c., but will be the same as if N was simply resolved into the factors a, b, c, &c.; and is, therefore, equal to

$$\frac{(1+1).(1+1).(1+1), \text{ \&c.}}{2}:$$

hence, if k represents the number of prime factors, a, b, c, d, &c., then will 2^{k-1} be the number of ways in which N may be resolved into two factors prime to each other. Thus, for example, 360 has twenty-four divisors (example 1), and, consequently, may be resolved into factors twelve different ways (cor. 2); but it has only three prime factors, 2, 3, and 5, and can, therefore, be resolved into factors prime to each other only, $2^2 = 4$, different ways.

PROP. II.

22. To find a number that shall have any given number of divisors.

Let w represent the given number of divisors, and resolve w into factors, as $w = x \times y \times z$. Take $m = x - 1$, $n = y - 1$, $p = z - 1$, &c.; so shall

$$a^m b^n c^p, \text{ \&c.},$$

be the number required, as is evident from the

foregoing proposition, where a, b, c, &c., may be taken any prime numbers whatever.

Ex. Find a number that shall have thirty divisors.

First, $30 = 2 \times 3 \times 5$; that is, $x = 2$, $y = 3$, $z = 5$; or, $m = 1$, $n = 2$, $p = 4$; therefore,

$$a . b^2 c^4$$

is the number, having thirty divisors, as required.

If $a = 2$, $b = 3$, $c = 5$; then $2 \,.\, 3^2 \,.\, 5^4 = \cancel{4608}$. 11250

If $a = 5$, $b = 3$, $c = 2$; then $5 \,.\, 3^2 \,.\, 2^4 = 720$.

If $a = 5$, $b = 2$, $c = 3$; then $5 \,.\, 2^2 \,.\, 3^4 = 1620$.

Each of which numbers has thirty divisors, and it is evident, that various other numbers might be obtained that would have the same property, by only changing the value of a, b, and c.

Remark. If it were required to find the least number of all those that have a given number of divisors, it is manifest, that we must proceed with more caution, as our formula would not then have that unlimited form that is given above. It will, therefore, be proper to enter, here, into an investigation of this particular case.

First, it is evident, that the value of our number depends upon two different operations: 1st, the resolution of w into its factors, which in the foregoing problem is arbitrary; and, 2dly, on the assumption of the quantities a, b, c, &c.

Now if w be a prime number, it cannot be resolved into any other factors than $1 \times w$; and, therefore, a^{w-1} is the only form a number can have when the number of its divisors is a prime number; and, therefore, the less value we give to $a > 1$, the

less the number will be: and, consequently, the least of all is when $a=2$; thus, the least number that has seven divisors is $2^6=64$, and the least having eleven divisors is $2^{10}=1024$, and so on.

Again, when w is not a prime number, but equal to the product of two prime factors, as $w=xy$, then the only variation in its resolution will be $w=x \times y$, and $w=1 \times xy$; and, consequently, the only two forms of numbers will be $a^{x-1}b^{y-1}$, and a^{xy-1}, that have the required number of divisors, and it is obvious that the first form is that which gives the least value of the number required; because a may, in both forms, be equal to 2, and b may be taken equal to 3; and, whatever be the numbers x and y, it is evident, that $2^{x-1} \times 3^{y-1} < 2^{xy-1}$: for if even we make $b=4$, in which case $2^{x-1} \times 4^{y-1}=(2)^{x+2y-3}$, it is still less than 2^{xy-1}, for $(x+2y-2) < xy$, because both x and y are >1, and x may also be supposed the greater of the two, that is, $x>y$. Therefore, $a^{x-1}b^{y-1}$ is that form which produces the least numbers, and it is manifest, that the least numbers in this form are those in which $a=2$, and $b=3$, $x-1$ being supposed the greatest exponent; and, in the same manner, it may be shown, that if w be resolvible into any number of factors, that will be the least form, in which w is resolved into the greatest number of factors, and the lowest number of any such form, as $a^m b^n c^p$, &c., is obviously that in which the greatest exponent has the least root, the next greater exponent the next less root, and so on. Therefore, when it is required to find the least number that has a given number of divisors, we must resolve the given number into its greatest

number of factors, and then proceed in given values to a, b, c, &c., according to the rule above given; *viz.* to the greatest exponent, the least root, &c. Suppose, for example, it were required to find the least number that has twenty divisors. The greatest number of factors is when $20 = 2 \times 2 \times 5$; therefore, $a^1 b^1 c^4$ is the least form: and by making $c = 2$, $b = 3$, $a = 5$, we have $2^4 . 3 . 5 = 240$, which is the least number of all those that have twenty divisors. If we had resolved 20 into the factors 4 and 5, then $a^4 b^3$ would have been the form, and, by making $a = 2$ and $b = 3$, we should have had $2^4 3^3 = 432$, for the least number in that form; and the same for all others.

PROP. III.

23. If $N = a^m b^n c^p$, &c., represent any integer, then will the sum of all the divisors of N be expressed by the formula

$$\left(\frac{a^{m+1} - 1}{a - 1}\right) \times \left(\frac{b^{n+1} - 1}{b - 1}\right) \times \left(\frac{c^{p+1} - 1}{c - 1}\right), \text{ \&c.}$$

For, by art. 21, every divisor of N is contained in the product

$$(1 + a + a^2, \text{ \&c., } a^m) \times (1 + b + b^2, \text{ \&c., } b^n) \times$$
$$(1 + c + c^2, \text{ \&c., } c^p) \times (1 + d + d^2, \text{ \&c, } d^q).$$

And, by the common rule for summing a geometrical progression, we have

$$1 + a + a^2 \text{ - - - } a^m = \frac{a^{m+1} - 1}{a - 1},$$

$$1 + b + b^2 \text{ - - - } b^n = \frac{b^{n+1} - 1}{a - 1}, \text{ \&c.};$$

and, consequently, this product is equal to

$$\left(\frac{a^{m+1}-1}{a-1}\right)\times\left(\frac{b^{n+1}-1}{b-1}\right)\times\left(\frac{c^{p+1}-1}{c-1}\right)\ \&c.,$$

which, therefore, expresses the sum of all the divisors of N. — Q. E. D.

Cor. In this expression, N is considered as a divisor of itself; because, from the developement of the above product, the last term will evidently be $a^m b^n c^p$, &c.; that is, the last term of the product will be the number N itself; and, therefore, when N is to be excluded by the condition of the problem, as is the case in finding perfect and amicable numbers, it must be deducted from the above formula.

Ex. Required the sum of all the divisors of 360.

First, $360 = 2^3 . 3^2 . 5$; therefore,

$$\left(\frac{2^4-1}{2-1}\right)\times\left(\frac{3^3-1}{3-1}\right)\times\left(\frac{5^2-1}{5-1}\right)=15.13.6=1170;$$

which is the sum of all the divisors of 360, itself being considered as one of them.

PROP. IV.

24. If $N = a^m b^n c^p$&c., represent any number, a, b, c, &c., being its prime factors, then will

$$N\times\frac{a-1}{a}\times\frac{b-1}{b}\times\frac{c-1}{c},\ \&c.,$$

express the number of integers that are less than N, and also prime to it.

First, if N be a prime number, or $N = a$, then we know, that all numbers less than a are also prime to it; and, consequently, $N\times\frac{a-1}{a} = a-1$ is the real expression for the number of them in this case.

And if N be any power of a prime number, or $N = a^m$, then, in the series of numbers

$$1,\ 2,\ 3,\ 4,\ 5,\ \&c.,\ a^m,$$

every *ath* term is a multiple of a, these forming of themselves the series

$$a,\ 2a,\ 3a,\ 4a,\ 5a,\ \&c.,\ a^{m-1}.\ a;$$

and, therefore, from the a^m terms in the first series, we must deduct the a^{m-1} terms in the last, and the remainder will be the number of those terms in the first, that are prime to N, or to a^m; that is, $a^m - a^{m-1}$ are the number of integers prime to N; but since $N = a^m$ we have

$$a^m - a^{m-1} = a^m \times \frac{a-1}{a} = N \times \frac{a-1}{a},$$

for the number of those integers, which is likewise the form in question.

Again, if $N = a^m b^n$, it is evident, from the same consideration as before, that we shall have

$a^{m-1}b^n$, terms divisible by a;
$a^m b^{n-1}$, terms divisible by b;
$a^{m-1}b^{n-1}$, terms divisible by ab.

But as the first expression includes all numbers divisible by a, and the second all those divisible by b, it follows, that the latter expression is included in each of the former; and, therefore, we have

$a^{m-1}b^n - a^{m-1}b^{n-1}$, terms divisible by a only;
$a^m b^{n-1} - a^{m-1}b^{n-1}$, terms divisible by b only;
$a^{m-1}b^{n-1}$, terms divisible by ab:

and these, together, include all those terms of the series

$$1,\ 2,\ 3,\ 4,\ 5,\ \&c.,\ a^m b^n,$$

that have any common divisor with $a^m b^n$, or with N; and, consequently, their sum, taken from N, will be the number of those that are prime to it: hence, then, we have

$$a^m b^n - a^{m-1} b^n - a^m b^{n-1} + a^{m-1} b^{n-1} =$$
$$(a^m - a^{m-1}) b^n - (a^m - a^{m-1}) b^{n-1} =$$
$$(a^m - a^{m-1}) \times (b^n - b^{n-1}) =$$
$$\left(a^m \times \frac{a-1}{a}\right) \times \left(b^n \times \frac{b-1}{b}\right) = \text{N} \times \frac{a-1}{a} \times \frac{b-1}{b},$$

which is again the formula in question.

Let, now, $\text{N} = a^m b^n c^p$, then, on the same principles as above, we shall have

$\text{P} = a^{m-1} b^n c^p$, terms divisible by a;
$\text{Q} = a^m b^{n-1} c^p$, terms divisible by b;
$\text{R} = a^m b^n c^{p-1}$, terms divisible by c;
$\text{S} = a^{m-1} b^{n-1} c^p$, terms divisible by ab;
$\text{T} = a^{m-1} b^n c^{p-1}$, terms divisible by ac;
$\text{V} = a^m b^{n-1} c^{p-1}$, terms divisible by bc;
$\text{W} = a^{m-1} b^{n-1} c^{p-1}$, terms divisible by abc.

But since all the terms W are necessarily included in those of S, T, and V; and these last again in P, Q, and R, we shall have, by subtraction,

S − W, divisible by ab only;
T − W, divisible by ac only;
V − W, divisible by bc only:

and then again,

P − S − T + 2W − W; or,
P − S − T + W, divisible by a only;
Q − S − V + W, divisible by b only;
R − T − V + W, divisible by c only;
W, divisible by abc only.

And, consequently, the sum of all these expressions will be the number of terms that have a common divisor with $a^m b^n c^p$, or with N; and, therefore, N *minus* this sum will be the number of integers prime to N, and less than itself; which, by addition and subtraction, will be expressed as follows:

$$N - P - Q - R + S + T + V - W.$$

And by reestablishing again the values of P, Q, R, &c., it becomes

$$(a^m b^n c^p - a^{m-1} b^n c^p) - (a^m b^{n-1} c^p - a^{m-1} b^{n-1} c^p) -$$
$$(a^m b^n c^{p-1} - a^{m-1} b^n c^{p-1}) + (a^m b^{n-1} c^{p-1} - a^{m-1} b^{n-1} c^{p-1}) =$$
$$(a^m - a^{m-1})(b^n c^p - b^{n-1} c^p - b^n c^{p-1} + b^{n-1} c^{p-1}) =$$
$$(a^m - a^{m-1}) \times (b^n - b^{n-1}) . (c^p - c^{p-1}) =$$
$$N \times \frac{a-1}{a} \times \frac{b-1}{b} \times \frac{c-1}{c},$$

the same form as before.

And, exactly in the same manner, if N was the product of a greater number of factors, we should still find, that the number of integers less than, and prime to N, would be represented by

$$N \times \frac{a-1}{a} \times \frac{b-1}{b} \times \frac{c-1}{c} \times \frac{d-1}{d}, \text{ \&c.}$$

Where it is only necessary to observe, that unity is included as one of those integers. — Q. E. D.

Ex. 1. Find how many numbers there are under 100, that are prime to it.

First, $100 = 2^2 5^2$; therefore,

$$100 \times \frac{2-1}{2} \times \frac{5-1}{5} = 40,$$

the number sought: these being as follows; *viz.*

1	13	27	39	51	63	77	89
3	17	29	41	53	67	79	91
7	19	31	43	57	69	81	93
9	21	33	47	59	71	83	97
11	23	37	49	61	73	87	99.

Ex. 2. How many numbers are there less than 360, that are also prime to it?

$$360 = 2^3 3^2 5\text{; therefore,}$$

$$360 \times \frac{2-1}{2} \times \frac{3-1}{3} \times \frac{5-1}{5} = 96,$$

the number sought.

PROP. V.

25. To find a perfect number, or such a number N, that shall be equal to the sum of all its aliquot parts, or divisors.

Find $2^n - 1$, a prime number, then will $2^{n-1}(2^n - 1) = N$ be a perfect number.

For, by art. 23, and its corollary, the sum of the divisors of the formula $2^{n-1}(2^n - 1)$ will be represented by

$$\left(\frac{2^n - 1}{2 - 1}\right) \times \left(\frac{(2^n - 1)^2 - 1}{(2^n - 1) - 1}\right);$$

because $2^n - 1$ is a prime number by hypothesis. But, in this expression, 1 is considered as a divisor, and, consequently, N enters therein as an aliquot part of itself, which is to be excluded by the definition of a perfect number; and, therefore, exclusive of N, the formula becomes

$$\left(\frac{2^n-1}{2-1}\right)\times\left(\frac{(2^n-1)^2-1}{(2^n-1)-1}\right)-2^{n-1}(2^n-1)=$$
$$(2^n-1)\times(2^n-1+1)-2^{n-1}(2^n-1)=$$
$$2(2^n-1)\,.\,2^{n-1}-2^{n-1}(2^n-1)=2^{n-1}(2^n-1)=\text{N};$$

that is, the sum of all the aliquot parts of $\text{N}=\text{N}$, and, therefore, it is a perfect number. — Q. E. D.

Cor. If

$n=2$, then $2\,(2^2-1)=6$;
$n=3$, then $2^2\,(2^3-1)=28$;
$n=5$, then $2^4\,(2^5-1)=496$;
$n=7$, then $2^6\,(2^7-1)=8128$;
$n=13$, then $2^{12}(2^{13}-1)=33550336$;
$n=17$, then $2^{16}(2^{17}-1)=8589869056$;
$n=19$, then $2^{18}(2^{19}-1)=137438691328$;
$n=31$, then $2^{30}(2^{31}-1)=2305843008139952128$.

Which are all perfect numbers.

The difficulty, therefore, of finding perfect numbers, arises from that of finding prime numbers, of the form 2^n-1, which is very laborious. Euler ascertained, that $2^{31}-1=2147483647$ is a prime number; and this is the greatest at present known to be such, and, consequently, the last of the above perfect numbers, which depends upon this, is the greatest perfect number known at present, and probably the greatest that ever will be discovered; for, as they are merely curious without being useful, it is not likely that any person will attempt to find one beyond it. It may not be amiss to observe, that the reason for employing the powers of 2 in this research, to the exclusion of all other numbers, arises from this, that 2 is the only even prime; and, therefore, if we made use of any other

prime, as a, then $(a^n - 1)$ would not be a prime number; and, if we employed an even number, then the formula above given would not truly express the sum of the divisors of N.

PROP. VI.

26. To find a pair of amicable numbers N and M, or such a pair of numbers, that each shall be respectively equal to all the divisors of the other.

Make $N = a^m b^n c^p$, &c., and $M = \alpha^u \beta^v \gamma^\pi$, &c.; then, from the definition of amicable numbers, and what has been demonstrated (art. 23), it follows that we must have

$$\left(\frac{a^{m+1}-1}{a-1}\right) \times \left(\frac{b^{n-1}-1}{b-1}\right) \times \left(\frac{c^{p+1}-1}{c-1}\right) = N + M, \text{ and}$$

$$\left(\frac{\alpha^{u+1}-1}{\alpha-1}\right) \times \left(\frac{\beta^{v+1}-1}{\beta-1}\right) \times \left(\frac{\gamma^{\pi+1}-1}{\gamma-1}\right) = M + N.$$

Because these formulæ include the whole numbers N and M, as divisors of themselves (*Remark*, art. 23), whereas, in amicable numbers, they are excluded by the definition.

We see, therefore, in order that the numbers N and M may be amicable, that these formulæ must be equal to each other, and each equal to N + M. Now this is accomplished by finding such a power of 2 as 2^r, that $3.2^r - 1$, $6.2^r - 1$, and $18.2^{2r} - 1$, may be all prime numbers; or, making $2^r = w$, we must have $3w - 1 = b$, $6w - 1 = c$, and $18w^2 - 1 = d$, all prime numbers; then will

$$N = 2^{r+1} d, \text{ and } M = 2^{r+1} bc,$$

be the pair of amicable numbers sought.

For, if we represent ϕN the sum of the divi-

sors of N, and by ϕM the sum of the divisors of M, we shall have (by cor. 1, art. 23)

$$\phi N = \left(\frac{2^{r+2}-1}{2-1}\right) \times \left(\frac{d^2-1}{d-1}\right) - 2^{r+1}d =$$
$$(2^{r+2}-1) \times (d+1) - 2^{r+1}d =$$
$$(4w-1) \times 18w^2 - 2w(18w^2-1) =$$
$$2 \,.\, 18w^3 - 18w^2 + 2w = 2w(3w-1)(6w-1) =$$
$$2^{r+1}bc = M.$$

Therefore the sum of the divisors of N is equal to the other number M.

And again, by the same art. and cor., we have

$$\phi M = \left(\frac{2^{r+2}-1}{2-1}\right) \times \left(\frac{b^2-1}{b-1}\right) \times \left(\frac{c^2-1}{c-1}\right) - 2^{r+1}bc =$$
$$(2^{r+2}-1) \times (b+1) \times (c+1) - 2^{r+1}bc =$$
$$(4w-1) \times 3w \times 6w - 2w(3w-1) \times (6w-1) =$$
$$18w^2(4w-1) - 2w(18w^2-9w+1) =$$
$$2w \times 18w^2 + 1 = 2^{r+1}d = N.$$

Therefore, the sum of the divisors of $M = N$; and we have seen, that the sum of the divisors of $N = M$: consequently, N and M are a pair of amicable numbers. — Q. E. D.

Scholium. By making $r=1$, or $2^r = w = 2$, we have $3w-1=b=5$, $6w-1=c=11$, and $18w^2-1=d=71$; and, consequently,

$$2^{r+1}d = 4 \times 71 = 284 = N,$$
$$2^{r+1}bc = 4 \times 5 \times 11 = 220 = M,$$

which are the least pair of amicable numbers, the next two pair being

17296 and 18416,
9363583 and 9437056.

The difficulty, therefore, of finding amicable numbers, is connected with that of finding the above specified conditions of w, and for which no rule has yet been discovered. The reason for taking w some power of 2 is, that 2 is the only even prime; for if w was the power of any odd number, then $3w-1$, $6w-1$, $18w^2-1$, would not be primes, and if w was the power of an even number, not a prime, as $2m$, then

$$\left(\frac{(2m)^{r+2}-1}{2m-1}\right)\times\left(\frac{b^2-1}{b-1}\right)\times\left(\frac{c^2-1}{c-1}\right)$$

would not be the true expression for the sum of the divisors of M: and, therefore, 2 is the only number that can be employed for this purpose.

PROP. VII.

27. If the *nth* term of any order of figurate numbers be added to the $n+1$ term of the next inferior order, the sum will be the $n+1$ term of the same order as the former. And the *nth* term of any order is equal to the n first terms of the preceding order.

In our definition of figurate numbers, we have given the form of each of the orders, because it is more simple to deduce the generation of figurate numbers from the form of them, than to deduce their forms from their generation. We have, therefore, to demonstrate, that the numbers falling under the forms we have given are generated one from another, as announced in this proposition; and this will be manifest immediately, by repeating

here again those series of figurate numbers, and their general terms, as given at definition 26; *viz.*

	General term.
Nat. series, 1 2 3 4 5, &c.	n
1st ord. 1 3 6 10 15, &c.	$\frac{n.(n+1)}{1\ .\ 2}$
2d ord. 1 4 10 20 35, &c.	$\frac{n.(n+1).(n+2)}{1\ .\ 2\ .\ 3}$
3d ord. 1 5 15 35 70, &c.	$\frac{n.(n+1).(n+2).(n+3)}{1\ .\ 2\ .\ 3\ .\ 4.}$

mth order, $\frac{n.(n+1).(n+2).(n+3),\ \&c.,\ (n+m)}{1\ .\ 2\ .\ 3\ .\ 4,\ \&c.,\ (m+1)}$.

Now it is evident, that $n+1$, which is the $n+1th$ term of the natural series, being added to $\frac{n.(n+1)}{1\ .\ 2}$, which is the *nth* term of the first order, gives

$$\frac{n.(n+1)}{1\ .\ 2}+n+1=\frac{(n+1).(n+2)}{1\ .\ 2},$$

which is the $n+1th$ term of the first order.

Again, to $\frac{n.(n+1).(n+2)}{1\ .\ 2\ .\ 3}$, the *nth* term 2d order, adding $\frac{(n+1).(n+2)}{1\ .\ 2}$, the $n+1th$ term 1st order, gives $\frac{(n+1).(n+2).(n+3)}{1\ .\ 2\ .\ 3}$, the $n+1th$ term 2d order.

And, generally, to

$$\frac{n.(n+1).(n+2).(n+3)\ -\ -\ -\ (n+m)}{1\ .\ 2\ .\ 3\ .\ 4\ -\ -\ -\ (m+1)}=nth\ \text{term}$$

mth order, adding

$$\frac{(n+1).(n+2).(n+3).(n+4) \; - - - \; (n+m)}{1 \; . \; 2 \; . \; 3 \; . \; 4 \; - - - \; m} = n+1th$$

term $m-1th$ order, gives

$$\frac{(n+1).(n+2).(n+3).(n+4) \; - - \; (n+1+m)}{1 \; . \; 2 \; . \; 3 \; . \; 4 \; - - - \; m+1} = n+1th$$

term mth order.

Hence, then, we have the general law of formation; namely, to the nth term of any order, add the $n+1$ term of the inferior order, and the sum will be the succeeding term of the former order. And, therefore, since the second term of any order is equal to the sum of the two first terms of the next inferior order, the third term will be equal to the sum of the three first terms of the preceding order; and, generally, the nth term of any order is equal to the sum of the first n terms of the next inferior order. — Q. E. D.

Scholium. In this proposition we have, after Legendre, inverted the order of proceeding, by deducing the law of generation from the forms of the successive series, instead of ascertaining the forms of those series from their law of generation, which has the advantage of greater simplicity, and leads us at once to the demonstration of one of Fermat's theorems, that he considered as one of his principal numerical propositions, and which is this:

If the nth term of the natural series be multiplied by the $n+1th$ term of any order m, the product will be equal to $m+2$ times the nth term of the order $m+1$.

Thus, taking the fifth and sixth term, of the foregoing series, we have

$5 \times 6 = 2 \times 15$; $5 \times 21 = 3 \times 35$; $5 \times 56 = 4 \times 70$, &c.

This property is deduced immediately from our forms, for

$$n(n+1)=2\times\frac{n.(n+1)}{1\;.\;2};$$

$$n\times\frac{(n+1).(n+2)}{1\;.\;2}=3\times\frac{n.(n+1).(n+2)}{1\;.\;2\;.\;3};$$

and so on for any other order.

This theorem, which is so remarkable simple in the way that we have considered these numbers, is very difficult to demonstrate by any other method; and that Fermat considered it as one of his most interesting propositions is evident, from what he says after the annunciation of it: "*Nec existimo pulchrius aut generalius in numeris posse dari theorema, cujus demonstrationem margini inserere nec vacat nec licet*" (Notes on Diophantus, page 16).

PROP. VIII.

28. Every polygonal number of the denomination m, or every m-gonal number, is expressed by the formula

$$\frac{(m-2)n^2-(m-4)n}{2}.$$

For, by definition 26, every m-gonal number is a sum of an arithmetical progression, beginning with unity, the common difference of which is $m-2$; or, making $m-2=d$, it will be the sum of any number n terms of the series

$$1+(1+d)+(1+2d)+(1+3d), \&c., (1+(n-1)d);$$

which, by the common rules, is equal to

$$\frac{(2+(n-1)d)n}{2},$$

or, since $d=m-2$, if we substitute for d, we shall have

$$\frac{(2+(n-1).d)n}{2}=\frac{2n+(n^2-n).(m-2)}{2}=$$
$$\frac{(m-2)n^2-(m-4)n}{2}. \qquad \text{Q. E. D.}$$

Cor. 1. Hence, by making successively $m=3, 4, 5$, &c., we shall have the following results. All

Triangular numbers $= \frac{n^2+n}{2}$.

Squares - - - - - $= \frac{2n^2-on}{2}=n^2$.

Pentagonals - - $= \frac{3n^2-n}{2}$.

Hexagonals - - $= \frac{4n^2-2n}{2}$.

&c. &c.

Cor. 2. By means of the general form

$$\frac{(m-2)n^2-(m-4)n}{2},$$

any polygonal number, of which the root n, and denomination m, is given, may be readily ascertained.

Thus, by making $m=3$, $m=4$, $m=5$, &c.; and in each series $n=1, 2, 3, 4$, &c., we have

Series of triang. numb.	1	3	6	10	15	21	28, &c.
Series of squares - -	1	4	9	16	25	36	49, &c.
Series of pentagons -	1	5	12	22	35	51	70, &c.
Series of hexagons -	1	6	15	28	45	66	91, &c.
&c.				&c.			

Also any polygonal number, and, its denomination being given, the root of the polygon is readily obtained. For let

$$P = \frac{(m-2)n^2 - (m-4)n}{2}$$

represent any given polygonal, of which the denomination m is known: then,

$$(m-2)n^2 - (m-4)n = 2P; \text{ or,}$$

$$n^2 - \left(\frac{m-4}{m-2}\right)n = \frac{2P}{m-2}. \quad \text{Whence}$$

$$n = \frac{m-4 \pm \sqrt{2P(m-2)+(m-4)^2}}{2m-4},$$

which is a general form for the root of any polygonal number.

Remark. Fermat has given, at page 15, in one of his notes to the ninth proposition of Diophantus on Multangular Numbers, particular rules for finding the roots of given polygonals, without the extraction of the square root, but, as they are of little or no use, we have not inserted them.

CHAP. III.

On the Forms of Prime Numbers, and their most simple Properties.

PROP. I.

29. If a number cannot be divided by some other number, which is equal to, or less than, the square root of itself, that number is a prime.

For every number p, that is not a prime, may be represented by $p=ab$. Now if $a=b$, then a and b are each equal to $\sqrt{p}$; and, consequently, p, which is not a prime, is divisible by $\sqrt{p}$. Again, if $a > \sqrt{p}$, then will $b < \sqrt{p}$; for otherwise, we should have $a \times b = ab > p$, which is contrary to the supposition; therefore, if $a > \sqrt{p}$, then will $b < \sqrt{p}$; and if $b > \sqrt{p}$, then will $a < \sqrt{p}$; and, consequently, since p is divisible both by a and b, it is divisible by a number less than the square root of itself: and this is evidently true of all numbers that can be resolved into the form $p=ab$; that is, of all numbers that are not primes: therefore, if a number cannot be so divided, that number is a prime. — Q. E. D.

Cor. Hence, in order to ascertain whether a given number be a prime number or not, we must attempt the division of it, by all the prime numbers less than the square root of itself; and if it be not divisible by any of them, it is a prime. It is obvious,

that we need only essay the division by prime numbers, for if it be divisible by a composite number, it is evidently also divisible by the prime factors of that divisor. This method, however, although it admits of some contractions, is, notwithstanding, extremely laborious for large numbers; nor has any easy, practical rule been yet discovered, for ascertaining whether a given number be a prime or not.

Scholium. The problem of finding prime numbers, was agitated so far back as the time of Eratosthenes, who invented what he called his κοσκινον, or *sieve*, for excluding those numbers that are not prime, and, consequently, thus discovering those that are. The principle of this method, which is the same that has since been employed by modern writers for ascertaining those numbers, is as follows:

Having written down in their proper order all odd numbers, from 1 to any extent, required; as

1	3	5	7	$\dot{9}$	11	13	$\ddot{15}$	17	19
$\ddot{21}$	23	$\dot{25}$	$\dot{27}$	29	31	$\dot{33}$	$\ddot{35}$	37	$\dot{39}$
41	43	$\ddot{45}$	47	$\dot{49}$	$\dot{51}$	53	$\dot{55}$	$\dot{57}$	59
61	$\ddot{63}$	$\dot{65}$	67	$\dot{69}$	71	73	$\ddot{75}$	$\dot{77}$	79
$\dot{81}$	83	$\dot{85}$	$\dot{87}$	89	$\dot{91}$	$\dot{93}$	$\dot{95}$	97	$\dot{99}$.

We begin with the first prime number 3, and over every third number, from that place, we put a point, because all those numbers are divisible by 3; as 9, 15, 21, &c.

Then, from 5, a point is placed over every fifth number, all these being divisible by 5; such are 15, 25, 35, &c.

Again, from 7 every seventh number is pointed in the same manner, such as 21, 35, 49, &c.

And, having done this, all the numbers that now remain without points are prime numbers; for there is no prime number between 7 and $\sqrt{100}$; and it is obvious, from what is said in the preceding corollary, that it is useless trying any composite number; adding, therefore, to the above, the prime number 2, which is the only even prime, we have

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97,					

which are all the prime numbers under 100.

By this means, assisted, probably, by some mechanical contrivance, Vega has computed, and published, a table of those numbers from 1 to 400000. And as it will be sometimes useful in the following part of this work, to know whether a given number be prime or not, without the trouble of computing it, a table is given at the end of this volume, exhibiting all the prime numbers from 2 to 10000.

PROP. II.

30. Every prime number, greater than 2, is of one of the forms $4n + 1$, or $4n - 1$.

For every number whatever is either divisible by 4, or, when the division by 4 is carried on as far as possible, there will be a remainder, 1, 2, or 3; that is, every number whatever is included under one or other of the four forms

$$4n, \; 4n + 1, \; 4n + 2, \; 4n + 3,$$

But the first and third of these forms are even numbers, being of the form $2n$, and, therefore, cannot contain any prime number > 2; and, consequently, all prime numbers greater than 2, are contained in the other two forms; and, therefore, every prime number is found in one or other of the two forms $4n+1$, or $4n+3$; but $4n+3 = 4(n+1) - 1, \doteqdot 4n-1$; therefore every prime number is of one of the forms $4n \pm 1$. — Q. E. D.

Cor. 1. Every prime number being of one of the forms $4n+1$, or $4n-1$, and as n, in these forms, must be either even or odd, we may subdivide them into the four following forms:

1. If n be even, or of the form $2n'$, $\begin{cases} 4n+1 \doteqdot 8n'+1; \\ 4n-1 \doteqdot 8n'-1 \doteqdot 8n''+7. \end{cases}$

2. If n be odd, or of the form $2n'+1$, $\begin{cases} 4n+1 \doteqdot 8n'+5; \\ 4n-1 \doteqdot 8n'+3. \end{cases}$

Hence all prime numbers, greater than 2, with regard to 8 as a modulus, are of one of the forms

$$8n+1,\ 8n+3,\ 8n+5,\ \text{or } 8n+7.$$

Cor. 2. The two forms $4n \pm 1$, separate prime numbers into two principal divisions, that are found to possess very distinct properties, which will be the subject of our future investigations; we shall, therefore, in this place, only give a few of those numbers, under each form, in order to render this classification the more familiar to the reader.

Primes $\doteqdot 4n+1$, are 1 5 13 17 29 37 41 53, &c.

Primes $\doteqdot 4n-1$, are 3 7 11 19 23 31 43, &c.

The other four forms, also, which are obtained

in the foregoing corollary, and in which the above two are necessarily involved, lead, also, to another principal classification of prime numbers, each class possessing properties exclusively its own. Primes divided according to this modulus are as follows:

$8n+1$	- - -	1	17	41	73	89	97	113.
$8n+3$	- - -	3	11	19	43	59	67	83.
$8n+5$	- - -	5	13	29	37	53	61	101.
$8n+7$	- - -	7	23	31	47	71	79	103.

Which are evidently numbers distinct from each other, and, as we observed above, possess very distinct properties, highly curious and interesting, many of which are demonstrated in the following chapters.

PROP. III.

31. Every prime number, greater than 3, is of one of the forms $6n+1$, or $6n-1$.

For every number whatever is either exactly divisible by 6, or when the division is carried on as far as possible, there will be a remainder 1, 2, 3, 4, or 5; that is, every number whatever is of one of the forms $6n$, $6n+1$, $6n+2$, $6n+3$, $6n+4$, $6n+5$. But the first, third, and fifth, of those numbers, are divisible by 2, and the fourth is divisible by 3, and, therefore, no one of these forms can contain prime numbers greater than 3; and, consequently, all prime numbers, greater than 3, must belong to one of the other two forms $6n+1$, or $6n+5$; but $6n+5 \doteq 6n'-1$; therefore, every prime number, greater than 3, is of one of the forms $6n+1$, or $6n-1$.—Q. E. D.

Cor. Since every prime number is of one of the

forms $6n+1$, or $6n-1$, and as n, in these forms, must be either even or odd, these may be subdivided into the four following forms:

1. If $n \doteq 2n'$, - - - $\begin{cases} 6n+1 \doteq 12n'+1; \\ 6n-1 \doteq 12n'-1 \doteq 12n+11. \end{cases}$

2. If $n \doteq 2n'+1$, - $\begin{cases} 6n+1 \doteq 12n'+7; \\ 6n-1 \doteq 12n'+5. \end{cases}$

Hence every prime number, with regard to modulus 12, is of one of the four forms

$$12n+1,\ 12n+5,\ 12n+7,\ \text{or}\ 12n+11:$$

or, which is still the same, every prime number is of one of the forms 12 ± 1, or $12n \pm 5$.

Scholium. It should be observed here, that although all prime numbers are contained in one or other of the foregoing forms, derived from art. 30 and 31, we must not conclude that the converse of the proposition is true also; namely, that all numbers contained in these forms are prime numbers: this is evidently not the case in the form $4n+1$, if $n=6$; nor in $4n-1$, if $n=4$; and similar exceptions may be found for every other form that may be devised: in fact, no formula can be found that shall express prime numbers only, as appears from the following proposition.

PROP. IV.

32. No algebraical formula can contain prime numbers only.

Let $p+qx+rx^2+sx^3+$, &c., represent any general algebraical formula, and it is to be demonstrated, that such values may be given to x, that the formula in question shall not produce a prime number, whatever values are given to p, q, r, s, &c.

For suppose, in the first place, that, by making $x = m$, the formula

$$\text{P} = p + qm + rm^2 + sm^3 +, \&\text{c.},$$

is a prime number.

And, if now we assume $x = m + \phi\text{P}$, we have

$$\begin{array}{ll} p = & p \\ qx = & qm + q\phi\text{P} \\ rx^2 = & rm^2 + 2rm\phi\text{P} + r\phi^2\text{P}^2 \\ sx^3 = & sm^3 + 3sm^2\phi\text{P} + 3sm\phi^2\text{P}^2 + s\phi^3\text{P}^3 \end{array}$$

&c.

Or,

$$p + qx + rx^2 + sx^3 = (p + qm + rm^2 + sm^3 +, \&\text{c.}) + \text{P}(q\phi + 2rm\phi + 3sm^2\phi) + \text{P}^2(r\phi^2 + 3sm\phi^2) + s\phi^3\text{P}^3 = \text{P} + \text{P}(q\phi + 2rm\phi + 3sm^2\phi) + \text{P}^2(r\phi^2 + 3sm\phi^2) + s\phi^3\text{P}^3.$$

But this last quantity is divisible by P; and, consequently, the equal quantity

$$p + qx + rx^2 + sx^3 +, \&\text{c.},$$

is also divisible by P, and cannot, therefore, be a prime number. Hence, then, it appears, that, in any algebraical formula, such a value may be given to the indeterminate quantity, as will render it divisible by some other number; and, therefore, no algebraical formula can be found that contains prime numbers only. — Q. E. D.

Scholium. But although no algebraical formula can be found, that contains prime numbers only, there are several remarkable ones that contain a great many; thus $x^2 + x + 41$, by making successively $x = 0, 1, 2, 3, 4$, &c., will give a series 41, 43, 47, 53, 61, 71, &c., the first forty terms of which are prime numbers. The above formula is mentioned by Euler in the Memoirs of Berlin (1772, page 36).

We may likewise add the two following; *viz.* x^2+x+17, and $2x^2+29$, of which the former has seventeen of its first terms primes, and the latter twenty-nine.

Fermat asserted, that the formula 2^m+1 was always a prime, while m was taken any term in the series 1, 2, 4, 8, 16, &c.; but Euler found, that $2^{32}+1=641\times6700417$ was not a prime. These examples are sufficient for showing, how easily we are led into error from induction, and how little it is to be depended upon, in mathematical investigations.

PROP. V.

33. The number of prime numbers is infinite.

For if not, let the number of them be represented by n, and the greatest of all those primes by p, then it is evident, that the continued product of all the prime numbers, not exceeding p, as

$$2\,.\,3\,.\,5\,.\,7\,.\,11\; - - -\; p,$$

will be divisible by each of those numbers, and, therefore, if 1 be added to it, it will be divisible by no one of them; and, consequently, if the formula

$$(2\,.\,3\,.\,5\,.\,7\,.\,11\; - - -\; p)+1$$

be divisible by any prime number, it must be by one greater than p; and if it be not divisible by any prime whatever, it is itself a prime number, which is necessarily greater than p; therefore, in either case, we must have a prime number greater than p; and, consequently, p is not the greatest; neither is n the greatest number of them, and the same is true of all finite numbers p, and n;

therefore, the number of prime numbers is infinite*.— Q. E. D.

PROP. VI.

34. If a be any number whatever, and b, b', b'', &c., all those numbers that are less than $2a$, and also prime to it; then will all prime numbers be contained in one or other of the forms

$$4an \pm b,\ 4an \pm b',\ 4an \pm b'',\ \&c.$$

For every number, when divided by $4a$, will leave for a remainder one of the terms in the series

$$0,\ 1,\ 2,\ 3,\ 4,\ \&c.,\ 4a-1;$$

or, which is the same,

$$\pm 0,\ \pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \&c.,\ 2a.$$

But it is evident, that, when any one of these remainders has a common divisor with $4a$, the number contained under that form is not a prime number, it having the same common divisor as the remainder and modulus; rejecting, therefore, all those remainders that have divisors common with $4a$, and representing the others by b, b', b'', &c., it

* It has also been demonstrated by Legendre (art. 404, *Essai sur la Theorie des Nombres*), that every arithmetical progression, of which the first term and common difference are prime to each other, contains an infinite number of prime numbers. And, also, that if N represent any number, then will $\frac{N}{h.log N - 1.08366}$; be the number of prime numbers that are less than N, *very nearly*. We should have added here the demonstration of this very curious theorem, but that it depends upon a fluxional consideration, which could not be well introduced into an elementary work of this kind.

is manifest, that all prime numbers will be contained in the forms

$$4an \pm b, \quad 4an \pm b', \quad 4an \pm b'', \quad \&c.,$$

at least all those that exceed the prime factors of a.— Q. E. D.

Cor. 1. Hence we may deduce, generally, the forms obtained at art. 30 and 31; *viz.*

If $a = 1$, all prime numbers $\doteqdot 4n \pm 1$;

If $a = 2$, all prime numbers $\begin{cases} \doteqdot 8n \pm 1; \\ \doteqdot 8n \pm 3; \end{cases}$

If $a = 3$, all prime numbers $\begin{cases} \doteqdot 12n \pm 1; \\ \doteqdot 12n \pm 5; \end{cases}$

If $a = 4$, all prime numbers $\begin{cases} \doteqdot 16n \pm 1; \\ \doteqdot 16n \pm 3; \\ \doteqdot 16n \pm 5; \\ \doteqdot 16n \pm 7. \end{cases}$

The number of forms, therefore, to any particular modulus, depends upon the number of integers, that are less than half that modulus, and also prime to it; and we have shown (art. 24) how this number may always be ascertained. Suppose, for example, that $2N$ was the given modulus; make

$$N = a^m b^n c^p, \ \&c.; \text{ then}$$

$$N \times \frac{a-1}{a} \times \frac{b-1}{b} \times \frac{c-1}{c}, \ \&c.,$$

will represent the number of forms.

Thus, if the modulus was 60, then we have

$$30 = 2 \cdot 3 \cdot 5; \text{ and, consequently,}$$

$$30 \times \frac{2-1}{2} \times \frac{3-1}{3} \times \frac{5-1}{5} = 8,$$

the number of forms, which are as follows:

$60n \pm 1$	$60n \pm 17$
$60n \pm 7$	$60n \pm 19$
$60n \pm 11$	$60n \pm 23$
$60n \pm 13$	$60n \pm 29$.

And hence it appears, that those numbers are to be preferred for moduli, that have the least number of integers less and prime to themselves; as we thereby exclude a greater number of quantities, that are not primes; or, which is the same, we have thus a less number of formulæ for expressing those that are primes. For example, if instead of modulus 60, which has only eight forms, we had taken 61, as a modulus, we should have had thirty forms; and under these thirty forms, every number whatever, not divisible by 61, may be expressed; and, consequently, with this modulus, no number is excluded; and, therefore, no advantage gained by the classification.

Scholium. It may not be amiss, to add here a few remarks upon the probability of any number, falling under any one of the above forms, being a prime number, when taken between certain limits. In order to which, it will be proper to enumerate the number of prime numbers, under certain periods, as deduced from *Vega's Mathematical Tables*, in which are given all prime numbers, from 2 to 400000; and by means of which the following tablet has been formed; which exhibits, at one view, the number of primes under and between the limits of every 10000 numbers.

		No. of primes.
Under	10000	1230
	20000	2263
	30000	3246
	40000	4204
	50000	5134
	60000	6058
	70000	6936
	80000	7837
	90000	8713
	100000	9592
	150000	13849
	200000	17984
	250000	22045
	300000	25998
	350000	29977
	400000	33861

			No. of primes.
Between	10000 and	20000	1033
	20000	30000	983
	30000	40000	958
	40000	50000	930
	50000	60000	924
	60000	70000	878
	70000	80000	901
	80000	90000	876
	100000	150000	4257
	150000	200000	4135
	200000	250000	4061
	250000	300000	3953
	300000	350000	3979
	350000	400000	3884

Now the number of integers falling under one or other of the above eight forms to modulus 60, is, for every 10000, $\frac{10000 \times 8}{60} = 1333$; and out of this number, for the first 10000, there are 1230, which are really primes; whence the probability of a number being a prime that falls under one of the above forms is $\frac{1230}{1333}$, if it be under 10000.

	Probability.
If the number be between 10000 and 20000,	$\frac{1033}{1333}$
If the number be between 20000 and 30000,	$\frac{983}{1333}$
If the number be between 30000 and 40000,	$\frac{958}{1333}$
&c.	&c.

This calculation is made upon a supposition, that the number of primes, in the above eight forms, are equal to each other, which is not strictly true; such an hypothesis, however, may be assumed, in a rough estimation of this kind, without affecting, in any great degree, the truth of the result.

PROP. VII.

35. Three prime numbers cannot be in arithmetical progression, unless the common difference of them be divisible by $2 \times 3 = 6$; except 3 be the first of the prime numbers, in which case there may be three prime numbers in arithmetical progression, whose common difference is not divisible by 6, but there can be only three.

For all prime numbers greater than 3 are of one of the forms $6n + 1$, or $6n + 5$. Also, if the common difference be not divisible by 6, it must be of one of the forms $6m + 1$, $6m + 2$, $6m + 3$, $6m + 4$, or $6m + 5$; or it may be otherwise represented by $6m + r$, r being any one of the numbers 1, 2, 3, 4, or 5. And, therefore, three numbers in arithmetical progression will be, either

1st, $6n + 1$, $6(n + m) + r + 1$, $6(n + 2m) + 2r + 1$; or
2d, $6n + 5$, $6(n + m) + r + 5$, $6(n + 2m) + 2r + 5$.

And it is to be proved, that some one of these terms, in both series, is divisible by 2, 3, or 6; and, consequently, that they are not all primes.

First, let $r = 1, 2, 3, 4,$ or 5; then we have, in the first series,

$$\begin{cases} r + 1 = 2, \ 3, \ 4, \ 5, \text{ or } 6; \\ 2r + 1 = 3, \ 5, \ 7, \ 9, \text{ or } 11. \end{cases}$$

And here it is evident, that either $r + 1$, or the corresponding term $2r + 1$, is divisible by 2, 3, or 6; and, consequently, one of the three terms in the first series is also divisible by the same; and, therefore, they are not all three primes. And we are

led to the same result in the second series; for, by making $r=1, 2, 3, 4, 5$;

$$\begin{cases} r+5=6, 7, 8, 9, \text{ or } 10; \\ 2r+5=7, 9, 11, 13, \text{ or } 15. \end{cases}$$

Where, also, one or other of the two corresponding terms has a common measure with 6; and, therefore, these three terms are not all primes. Consequently there cannot be three prime numbers in arithmetical progression, unless their common difference be divisible by 6, if we except the case where the first term of the progression is 3. And in this case there can be only three, for otherwise, by taking away the first, there would still remain three prime numbers in arithmetical progression, of which the common difference is not divisible by 6, which is contrary to what has been demonstrated above. — Q. E. D.

PROP. VIII.

36. There cannot be five prime numbers in arithmetical progression, unless their common difference be divisible by $2 \times 3 \times 5 = 30$; except when the first term of the progression is 5, in which case there may be five prime numbers in arithmetical progression, whose common difference is not divisible by 30, but there can be no more than five.

For all prime numbers greater than 5 to modulus 30, are of one of the following forms:

$$30n+1, \; 30n+7, \; 30n+11, \; 30n+13,$$
$$30n+17, \; 30n+19, \; 30n+23, \; 30n+29.$$

And since, by the foregoing proposition, three

prime numbers cannot be in arithmetical progression, unless their common difference be divisible by 6, it follows *a fortiori*, that 5 cannot be so unless the common difference be also divisible by 6; therefore, the common difference, in this case, as compared with modulus 30, must be of one of the forms $30m+6$, $30m+12$, $30m+18$, or $30m+24$, all other forms being rejected as not being divisible by 6, which we have seen is a necessary condition. Assuming, therefore, $30n+r$ for a general expression for prime numbers, and $30m+6p$ a general expression for the common difference, our five terms of the progression will be

$$30n+r,$$
$$30(n+m)+r+6p,$$
$$30(n+2m)+r+12p,$$
$$30(n+3m)+r+18p, \text{ and}$$
$$30(n+4m)+r+24p.$$

Now it readily appears, that whatever value is given to r, of the above; *viz.* 1, 7, 11, 13, 17, 19, 23, or 29; and to p of those which it represents; *viz.* 1, 2, 3, or 4; one or other of the expressions $r+6p$, $r+12p$, $r+18p$, or $r+24p$, is divisible by one of the numbers, 2, 3, or 5. Thus,

If $r=1$, and $p=1$, then $r+24p \leftarrow$ *5.
If $r=1$, and $p=2$, then $r+12p \leftarrow$ 5.
If $r=1$, and $p=3$, then $r+18p \leftarrow$ 5.
If $r=1$, and $p=4$, then $r+6p \leftarrow$ 5.

And so on of any other values of p and r.

* This character signifies *divisible by*, and is only employed to save the repetition of those words.

Whence it follows, that these five numbers cannot be all prime numbers; that is, five prime numbers cannot be in arithmetical progression, unless their common difference be divisible by 30, if we except the case in which the first term of the progression is 5; which evidently is excepted in the demonstration, as our forms are for primes greater than 5. The two primes, 2 and 3, are also excepted; and, with regard to the first, it is evident it cannot form the first term of such a progression, because it is an even number; but 3 may be taken for a first term, and, by giving to r this value, the same impossibility will appear. There cannot, therefore, be five prime numbers in arithmetical progression, unless their common difference be divisible by $2 \times 3 \times 5$, excepting only the case where the first term is 5, and in this case there can be only five; for if there were six, by taking away the first, there would still remain five prime numbers in arithmetical progression, whose common difference would not be divisible by 30, which is contrary to what has been shown above. — Q. E. D.

Cor. In the same manner it may be demonstrated that seven prime numbers cannot be in arithmetical progression, unless their common difference be divisible by $2 \times 3 \times 5 \times 7 = 210$; except the first of those prime numbers be 7, in which case there may be seven prime numbers in arithmetical progression, of which the common difference is not divisible by 210, but there cannot be more than seven. And, generally, there cannot be n prime numbers in arithmetical progression, unless their common difference be divisible by

$2 \times 3 \times 5 \times 7 \times 11$, &c., n; except the case in which n is the first term of the progression, in which case there may be n such numbers, but not more.

PROP. IX.

37. The sum of any number of prime numbers in arithmetical progression is a composite number.

This is evidently true, if the number of terms in the progression be an even number, because then their sum will be even, and, therefore, composite. We have, therefore, only to consider the case, in which the number of terms in the progression is odd. Let, then, p be the first prime number, and d the common difference of the progression; then, if we consider at first only three terms, they will be

$$p+(p+d)+(p+2d)=3p+3d,$$

which is evidently divisible by 3, and, therefore, a composite number. If we take five terms, they will be

$$p+(p+d)+(p+2d)+(p+3d)+(p+4d)= 5p+10d,$$

which is evidently divisible by 5; and, generally, we may assume

$$p+(p+d)+(p+2d)+, \&c., (p+2nd)$$

for any progression, the sum of which is

$$(2n+1)p+\frac{(1+2n)d \times 2n}{2}=(2n+1)p+(2n+1)nd;$$

it will be divisible by $2n+1$, and is, therefore, a composite number. — Q. E. D.

PROP. X.

38. If a and b be any two numbers prime to each other, and each of the terms of the series

$$b,\ 2b,\ 3b,\ 4b,\ ---\ (a-1)b,$$

be divided by a, they will each leave a different positive remainder.

For if any two of these terms, when divided by a, leave the same remainder, let them be represented by xb and yb, and their common remainder by r; so that $xb = na + r$, and $yb = ma + r$; then it is evident, that

$$xb - yb = na - ma$$

will be divisible by a. But this is impossible, for $xb - yb = b \times (x - y)$; in which product the factor b is prime to a, and $(x - y) < a$; because both x and y are less than a, by the hypothesis; consequently, their difference must be so; but if, of two factors, one be prime and the other less than a third number, the product is not divisible by this number (cor. 6, art. 11); therefore, $b \times (x - y)$ is not divisible by a; and, therefore, $xb = na + r$, and $yb = ma + r$, are impossible; that is, no two of those terms can leave the same remainder, when both are divided by a. — Q. E. D.

Cor. 1. Since, then, the remainders arising from the division of each of the terms in the series

$$b,\ 2b,\ 3b,\ 4b,\ ---\ (a-1)b,$$

by a, are different from each other and $a - 1$ in number, also all of them necessarily less than a; it follows, that these remainders include all numbers from 1 to $a - 1$.

Cor. 2. Hence, again, it appears, that some one of the above terms will leave a remainder 1; and that, therefore, if b and a be any two numbers prime to each other, a number $x < a$ may be found, that will render $bx - 1$ divisible by a; or, the equation $bx - ay = 1$ is always possible, if a and b are numbers prime to each other.

And it is always impossible if a and b have any common measure, as is evident; because one side of the equation, $bx - ay = 1$, would be divisible by this common measure; but the other side, 1, would not be so: therefore, in this case, the equation is impossible.

Cor. 3. We have seen, in the foregoing corollary, that the equation $bx - ay = 1$ is always possible, when a and b are prime to each other; and the same is evidently true of the equation $bx - ay = -1$, for $a - 1$ is one of the remainders in the above series, so that a value of $x < a$ may be found, that renders $bx - (a - 1)$ divisible by a; or the equation $bx - ay = a - 1$ is always possible; but this is the same as $bx - a(y - 1) = -1$; or, making $y - 1 = y'$, $bx - ay' = -1$ is always possible; and, consequently, the equation $ax - by = \pm 1$ is always possible, when a and b are prime to each other.

PROP. XI.

39. If a be any prime number, then will

$$1 . 2 . 3 . 4 . 5 \cdots (a-1) + 1$$

be divisible by a.

For, in cor. 2 of the foregoing proposition, it is demonstrated, that if a and b be any two numbers

prime to each other, another number x may be found $< a$, that renders the product $bx - 1 \div a$; or, which is the same thing, $bx = ya + 1$; and that there is only one such value of $x < a$ may be shown as follows:

The foregoing equation gives, by transposition,

$$bx - ay = 1;$$

and, if it be possible, let also

$$bx' - ay' = 1;$$

and make $x' = x \pm m$, and $y' = y \pm n$, where m is necessarily less than a, because both x and x' are so by the supposition. Now, by this substitution, we have

$$\begin{aligned} (bx \pm bm) - (ay \pm an) &= 1; \text{ but} \\ bx \qquad - ay \qquad &= 1; \end{aligned}$$

therefore $\pm bm = \mp an$, or $bm \div a$; but this is impossible, since b is prime to a, and $m < a$ (cor. 6, art. 11).

There cannot, therefore, be two values of x less than a, that renders the equation $bx - ay = 1$ possible.

But in the series of integers

$$1,\ 2,\ 3,\ 4,\ 5, \ldots\ a - 1,$$

every term is prime to a, except the first, a being itself a prime; if, therefore, we write successively, $b = 2$, $b' = 3$, $b'' = 4$, &c., a corresponding term x, in the same series, may be found for each distinct value of b, that renders the product $xb \doteq ay + 1$, $x'b' \doteq ay' + 1$, $x''b'' \doteq ay + 1$, &c.; and it is evident, that no one of these values of x can be equal either to 1, or $a - 1$; for, in the first case, we should have $1 \times b = ay + 1$, which is impossible, because $b < a$;

and the second would give $(a-1)b = ay+1$, or $a(b-y) = b+1$; that is, $b+1 \div a$; which can only be when $b = a-1$, or when $b = x$, which case is excepted, because we suppose two different terms of the series. In fact, since $(a-1)^2 \doteqdot ay+1$, there can be no other term, in the same series, that is of this form; for if $x^2 \doteqdot ay'+1$, then $(a-1)^2 - x^2$ would be divisible by a, or $(a-1+x) \times (a-1-x) \div a$, which is impossible, since each of these factors is prime to a, as is evident, because $x < a$, and a is a prime number.

Hence, then, our product

$$1 \,.\, 2 \,.\, 3 \,.\, 4 \,.\, 5 \text{ - - - } (a-1), \text{ becomes}$$
$$1 \,.\, bx \,.\, b'x' \,.\, b''x'' \text{ - - - } a-1;$$

but each of these products, bx, $b'x'$, $b''x''$, &c., is, as we have seen, of the form $ay+1$; therefore, their continued product will have the same form, and the whole product, including 1 and $a-1$, will be

$$\doteqdot (ay+1) \times (a-1) \doteqdot a^2y + ay + a - 1,$$

to which, if unity be added, the result will be evidently divisible by a, that is, the formula

$$1 \,.\, 2 \,.\, 3 \,.\, 4 \,.\, 5 \text{ - - - } (a-1)+1$$

is always divisible by a, when a is a prime number. — Q. E. D.

Cor. 1. The product,

$$1 \,.\, 2 \,.\, 3 \,.\, 4 \,.\, 5 \text{ - - - } (a-1),$$

is the same as

$$1(a-1)2(a-2)3(a-3), \text{ \&c.}, \left(\frac{a-1}{2}\right)^2;$$

and this product, with regard to its remainder, when divided by a, is the same as

$$\pm 1^2 . 2^2 . 3^2 . 4^2 \text{ - - - } \left(\frac{a-1}{2}\right)^2;$$

the ambiguous sign being *plus* $(+)$ when $a-1$ is even, and *minus* $(-)$ when $a-1$ is odd; that is, $+$ when a is a prime number of the form $4n+1$, and $-$ when a is a prime number of the form $4n-1$; also this product,

$$\pm 1^2 . 2^2 . 3^2 . 4^2 \text{ - - - } \left(\frac{a-1}{2}\right)^2,$$

is the same as

$$\pm\left(1 . 2 . 3 . 4 \text{ - - - } \frac{a-1}{2}\right)^2;$$

and, consequently, from what is said above relating to the ambiguous sign, we shall have

$$\left\{\left(1 . 2 . 3 . 4 \text{ - - - } \frac{a-1}{2}\right)^2 + 1\right\} \div a,$$

when $a \doteq 4n+1$; and

$$\left\{\left(1 . 2 . 3 . 4 \text{ - - - } \frac{a-1}{2}\right)^2 - 1\right\} \div a,$$

when $a \doteq 4n-1$.

Whence it follows, that every prime number of the form $4n+1$ is a divisor of the sum of two squares.

Again, the latter form may be resolved into the two factors

$$\left\{\left(1 . 2 . 3 . 4 \text{ - - - } \frac{a-1}{2}\right) + 1\right\} \times$$
$$\left\{\left(1 . 2 . 3 . 4 \text{ - - - } \frac{a-1}{2}\right) - 1\right\},$$

which product, being divisible by a, it follows,

that a is a divisor of one or other of these factors, when it is a prime number of the form $4n-1$.

Cor. 2. From the first product, which we have demonstrated to be divisible by a, *viz.*

$$\frac{1\,.\,2\,.\,3\,.\,4,\ \&c.,\ (a-1)+1}{a}=e,\ \text{an integer,}$$

we may derive a great many others; as

$$\frac{1^2.\,2^2.\,3\,.\,4\,.\,5,\ \&c.,\ (a-3)(a-1)+1}{a}=e,\ \text{an integer;}$$

$$\frac{1^2.\,2^2.\,3^2.\,4\,.\,5,\ \&c.,\ (a-4)(a-1)+1}{a}=e,\ \text{an integer;}$$

and so on, till we arrive at the same form as that in cor. 1.

Scholium. The theorem above demonstrated was invented by sir John Wilson, as we are informed by Waring, in his *Meditationes Algebraicæ,* page 380; but, notwithstanding the simple principles on which its demonstration is founded, it escaped the observation of these two celebrated mathematicians; the latter of whom speaks of it, at the place above quoted, as an extremely difficult proposition to demonstrate, on account of our having no formula for expressing prime numbers. Lagrange was the first who demonstrated this theorem, in the *New Memoirs of the Academy of Berlin,* 1771 (which demonstration is, as might be expected from the celebrity of its author, very ingenious); and, afterwards, Euler gave a different demonstration of the same proposition, in his *Opusc. Analyt.* tom. i. page 329, which is upon a similar

principle as the foregoing; and, finally, Gauss, in his *Disquisitiones Arithmeticæ*, extended the theorem by demonstrating, that "*The product of all those numbers less than, and prime to a given number* $a \pm 1$ *is divisible by* a;" the ambiguous sign being $-$, when a is of the form p^m, or $2p^m$, p being any prime number greater than 2; and, also, when $a = 4$; but positive in all other cases (*Recherches Arithmetiques*, page 57).

The theorem of sir John Wilson furnishes us with an infallible rule, *in abstracto*, for ascertaining whether a given number be a prime or not; for it evidently belongs exclusively to those numbers, as it fails in all other cases, but is of no use in a practical point of view, on account of the great magnitude of the product even for a few terms.

PROP. XII.

40. If a and b be any two numbers prime to each other, the equation

$$ax - by = \pm c$$

is always possible; and an infinite number of different values may be given to x and y, that answers the condition of the equation, in integer numbers.

For, by (cor. 3, art. 38) the equation,

$$ax - by = \pm 1$$

is always possible, while a and b are prime to each other; and, consequently,

$$acx - bcy = \pm c, \text{ or } ax' - by' = \pm c; \text{ by making}$$

$$cx = x', \text{ and } cy = y':$$

and we have evidently the same result if we write

$$a(x' \pm mb) \text{ for } ax', \text{ and}$$
$$b(y' \pm ma) \text{ for } by'; \text{ for these still give}$$
$$a(x' \pm mb) - b(y' \pm ma) = \pm c.$$

Or, again, making

$$x' \pm mb = x, \text{ and } y' \pm ma = y,$$

our equation becomes

$$ax - by = \pm c;$$

which is, therefore, always possible.

And it is evident, that by means of the ambiguous sign $\pm$, and the indeterminate quantity m, the formulæ

$$x' \pm mb = x,$$
$$y' \pm ma = y,$$

will furnish an infinite number of values of x and y, that answers the condition of the equation

$$ax - by = \pm c, \text{ in integers,}$$

a and b being prime to each other. — Q. E. D.

It is also obvious, that m may be so assumed, that x shall be less than b, or $y < a$.

Cor. Hence, in any of our future investigations, if we have two quantities, t and u, prime to each other, we may always substitute $tx - uy = c$, c being any number whatever, when the state of the question requires such a substitution, without considering the particular values of x and y, it being sufficient for our purpose, in many cases, to know that the equation is possible.

But if t and u have any common measure, then such a substitution cannot be made, unless c have the same common measure.

PROP. XIII.

41. The equation $ax+by=c$ is always possible, if a and b be prime to each other, and

$$c>(ab-a-b).$$

For let $c=(ab-a-b)+r$, then the equation becomes

$$ax+by=(ab-a-b)+r;$$

the possibility of which depends upon

$$x=\frac{ab-a-b-by+r}{a}$$

being an integer. Now this equation is the same as

$$x=b-1-\frac{(y+1)b-r}{a};$$

and, therefore, it depends upon the possibility of

$$\frac{(y+1)b-r}{a}=x' \text{ being an integer};$$

or, which is still the same, by calling $y+1=y'$, upon the possibility of the equation $y'b-ax'=r$; which we have seen may always be established, so that $y'<a$, or $y+1<a$; by the foregoing proposition.

Since, then, in the equation

$$\frac{(y+1)b-r}{a}=x',$$

$y+1$ is less than a, x' must necessarily be less than b, and, consequently,

$$x=b-1-\frac{(y+1)b-r}{a}=b-1-x';$$

and, since $x' < b$, therefore $x = b - 1 - x' = o$, or some integer number: whence the equation

$$ax + by = c$$

is always possible, when a and b are prime to each other, and $c > (ab - a - b)$. — Q. E. D.

Cor. The two foregoing propositions are very useful in judging of the possibility, or impossiblity, of indeterminate equations of this kind; and, consequently, also, in proposing them, so that they may be within possible limits.

CHAP. IV.

On the possible and impossible Forms of Square Numbers, and their Application to Numerical Propositions.

PROP. I.

42. Every square number is of one of the forms

$$4n, \text{ or } 4n+1.$$

For every number, being either even or odd, is of one of the forms $2n$, or $2n+1$; and, consequently, every square number is of one of the forms

$4n^2$, or $(4n^2+4n+1)$; but

$4n^2 \doteq 4n$, and

$(4n^2+4n+1)=4(n^2+n)+1 \doteq 4n+1$.

Q. E. D.

Cor. 1. Every square of the form $4n$ is necessarily even; and every square of the form $4n+1$ is evidently odd; therefore, every even square is of the form $4n$, and every odd square of the form $4n+1$.

Cor. 2. By the foregoing proposition it appears, that every odd square is of the form $4(n^2+n)+1$; and hence it follows, that it is also of the form $8n+1$: for if n be odd, n^2 is odd, and if n be even, n^2 is even also; therefore, in both cases, n^2+n is even; and, consequently, $4(n^2+n)+1 \doteq 8n+1$; that is, every odd square is of the form $8n+1$. If,

therefore, a number be of the form $4n+1$, but not of the form $8n+1$, that number is not a square.

Cor. 3. No numbers of the forms $4n+2$, or $4n+3$, can be square numbers. Nor can any numbers of the forms $8n+2$, $8n+3$, $8n+5$, $8n+6$, or $8n+7$, be square numbers.

Cor 4. The sum of two odd squares cannot form a square, for $(4n+1)+(4n'+1) \mp 4n+2$, which cannot be a square (cor. 3).

Cor. 5. An odd square, subtracted from an even square, cannot leave a square remainder. For

$$4n-(4n'+1)=4(n-n')-1 \mp 4n+3,$$

which cannot be a square. Therefore, if the difference of an even and odd square be a square, the odd square must be the greatest.

Cor. 6. If the sum of an even and odd square be a square, the even square must be divisible by 16, or be of the form 4^2n^2. For all odd squares are of the form $8n+1$ (cor. 2); and, therefore, if the even square had only the form $4n'^2$, n'^2 being odd, the sum of the two would be

$$4n'^2+8n+1=4(n'^2+2n)+1;$$

and since n'^2 is odd, (n'^2+2n) is odd also; and, therefore, $4(n'^2+2n)+1$ is not of the form $8n+1$; and, consequently, it is not a square (cor. 2).

PROP. II.

43. Every square number is of one of the forms

$$5n, \text{ or } 5n \pm 1.$$

For all numbers, compared by modulus 5, are of one of the forms $5n$, $5n \pm 1$, $5n \pm 2$; that is, every number is either divisible by 5, or will leave for a

remainder 1, 2, 3, or 4; or, which is the same, ± 1, or ± 2: and, consequently, all square numbers are of one of the following forms:

Numbers.	*Squares.*	*Forms.*
$5n$,	$25n^2$	$\doteqdot 5n$
$5n \pm 1$,	$25n^2 \pm 10n + 1$	$\doteqdot 5n + 1$
$5n \pm 2$,	$25n^2 \pm 20n + 4$	$\doteqdot 5n + 4 \doteqdot 5n - 1$.

Consequently, all square numbers are of one of the forms $5n$, or $5n \pm 1$. — Q. E. D.

Cor. 1. If a square number be divisible by 5, it is also divisible by 25; and, if a number be divisible by 5, and not by 25, it is not a square.

Cor. 2. No number of the form $5n + 2$, or $5n + 3$, is a square number.

Cor. 3. If the sum of two squares be a square, one of the three is divisible by 5, and, consequently, also by 25. For all the possible combinations of the three forms $5n$, $5n + 1$, and $5n - 1$, are as follows:

$$(5n + 1) + (5n' + 1) \doteqdot 5n + 2,$$
$$(5n - 1) + (5n' - 1) \doteqdot 5n - 2 \doteqdot 5n + 3,$$
$$5n + 5n' \doteqdot 5n,$$
$$5n + (5n' + 1) \doteqdot 5n + 1,$$
$$5n + (5n' - 1) \doteqdot 5n - 1,$$
$$(5n + 1) + (5n' - 1) \doteqdot 5n.$$

Now of these six forms, the latter four have one of the squares divisible by 5, and, therefore, also by 25 (cor. 1). And the two first are each impossible forms for square numbers; that is, neither of these two combinations can produce squares: therefore, if the sum of two squares be a square, one of the three squares is divisible by 25.

Cor. 4. By means of the two foregoing propositions, and their corollaries, it appears, that no number contained under a repetend digit can be a square number.

For every number expressed by a repetend digit is equal to the same number of repetend units, multiplied by the particular digit under the repetend of which the number is contained.

But every repetend of units is of the form

$$100n + 11 \doteqdot 4n + 3 \doteqdot 5n + 1\,;$$

and it is only necessary to show, that no number of the form $4n + 3$, or $5n + 1$, multiplied by any one of the nine digits, can be a square. Now the following products,

$$(4n + 3) \times 1,$$
$$(4n + 3) \times 4,$$
$$(4n + 3) \times 9,$$

cannot produce squares, because one of the factors is a square, and the other not; and, consequently, the product cannot be a square (art. 15).

Again,

$$(4n + 3) \times 2 \doteqdot 4n' + 2,$$
$$(4n + 3) \times 5 \doteqdot 4n' + 3,$$
$$(4n + 3) \times 6 \doteqdot 4n' + 2\,;$$

which are all impossible forms for squares (cor. 3, art. 42). And since a repetend unit is likewise of the form $5n + 1$, we have

$$(5n + 1) \times 3 \doteqdot 5n' + 3,$$
$$(5n + 1) \times 7 \doteqdot 5n' + 2,$$
$$(5n + 1) \times 8 \doteqdot 5n' + 3,$$

each of which is an impossible form (cor. 2, art. 43);

and, consequently, no repetend digit can be a square number. — Q. E. D.

Cor. 5. Every square number being of one of of the forms $5n$, or $5n \pm 1$; or, which is the same thing, of one of the three forms $5n$, $5n+1$, or $5n+4$; we may farther divide them into the following classes, according to modulus 10, by taking n even or odd:

$$5n \;\;\; \doteqdot 10n', \quad \text{when } n \text{ is even;}$$
$$5n \;\;\; \doteqdot 10n'+5, \quad \text{when } n \text{ is odd;}$$
$$5n+1 \doteqdot 10n'+1, \quad \text{when } n \text{ is even;}$$
$$5n+1 \doteqdot 10n'+6, \quad \text{when } n \text{ is odd;}$$
$$5n+4 \doteqdot 10n'+4, \quad \text{when } n \text{ is even;}$$
$$5n+4 \doteqdot 10n'+9, \quad \text{when } n \text{ is odd.}$$

Therefore, every square number, compared by modulus 10, is of one of the forms

$$10n,\ 10n+1,\ 10n+4,\ 10n+5,\ 10n+6,\ 10n+9.$$

And hence it follows, that all square numbers are terminated, on the right hand, by one of the digits 0, 1, 4, 5, 6, or 9. And, consequently, no number, whose last digit is 2, 3, 7, or 8, is a square number.

Cor. 6. By an examination of the first fifty square numbers to modulus 100, the following properties of the terminations of all squares will be readily deduced.

1. A square number cannot terminate with an odd number of ciphers.

2. If a square number terminate with a 4, the last figure but one will be an even number.

3. If a square number terminate with 5, it will terminate with 25.

4. If a square number terminate with an odd digit, the last figure but one will be even; and, if it terminate with any even digit, except 4, the last figure but one will be odd.

5. No square number can terminate with two equal digits, except two 0s or two 4s.

6. A square number cannot terminate with more than three equal digits, unless they be 0s; neither can it terminate in three, unless they be three 4s *.

PROP. III.

44. All square numbers are of the same form with regard to any modulus a, as the squares

$$0^2,\ 1^2,\ 2^2,\ 3^2,\ \&c., \text{ - - - } (\tfrac{1}{2}a)^2, \text{ when } a \text{ is even};$$

and as the squares

$$0^2,\ 1^2,\ 2^2,\ 3^2,\ \&c., \text{ - - - } \left(\frac{a-1}{2}\right)^2, \text{ when } a \text{ is odd}.$$

For every number may be represented by the formula $an \pm r$, in which r never exceeds $\frac{1}{2}a$ (cor. 2, art. 10). Now

$$(an \pm r)^2 = a^2n^2 \pm 2anr + r^2 = a(an^2 \pm 2nr) + r^2;$$

and, since the first part of this formula is divisible by a, the whole formula will leave the same remainder, when divided by a, as the part r^2; that is, it will be of the same form, with regard to the

* By means of these, and similar observations on the forms and terminations of square numbers, we may frequently ascertain, from inspection, whether a given number be a square or not, without the trouble of extraction.

modulus a, as the square r^2; but r never exceeds $\frac{1}{2}a$, therefore, all square numbers, as referred to modulus a, being of the same forms as the squares

$$0^2,\ 1^2,\ 2^2,\ 3^2,\ \&c., \text{ - - - } r^2,$$

in which r is limited not to exceed $\frac{1}{2}a$; it follows, that all square numbers, to modulus a, are of the same form as the squares

$$0^2,\ 1^2,\ 2^2,\ 3^2,\ \&c., \text{ - - - } (\tfrac{1}{2}a)^2, \text{ when } a \text{ is even};$$

and to the squares

$$0^2,\ 1^2,\ 2^2,\ 3^2,\ \&c., \text{ - - - } \left(\frac{a-1}{2}\right), \text{ when } a \text{ is odd.}$$

Q. E. D.

Cor. When a is even, the general formula

$$a^2n^2 \pm 2anr + r^2, \text{ becomes}$$
$$4a'^2n^2 \pm 4a'nr + r^2,$$
$$= 4a'(a'n^2 \pm nr) + r^2;$$

therefore, all square numbers are of the same form, to modulus $4a$, as the squares

$$0^2,\ 1^2,\ 2^2,\ 3^2,\ \&c., \text{ - - - } a^2.$$

And hence we see, immediately, that all squares, to modulus 8, are of the forms $8n$, $8n+1$, or $8n+4$, being all of the same form as the three squares

$$0^2,\ 1^2, \text{ and } 2^2.$$

45. *Scholium* 1. In order to ascertain the forms under which all square numbers are contained, with regard to any particular number a, as a modulus, we need only find the forms of all squares from 0^2 to $(\frac{1}{2}a)^2$, when a is even; or to $\left(\frac{a-1}{2}\right)^2$, when a is odd; and the results will necessarily include the forms under which every

square number whatever is contained: and thus the following table is very readily computed, which exhibits all the possible forms of square numbers, for every modulus from 2 to 20, and which may be continued to any length at pleasure.

Table of the Forms under which all Square Numbers are contained, for every Modulus from 2 to 20.

Moduli.	*Formulæ.*				
2	$2n$	$2n+1$			
3	$3n$	$3n+1$			
4	$4n$	$4n+1$			
5	$5n$	$5n\pm 1$			
6	$6n$	$6n+1$	$6n+3$	$6n+4$	
7	$7n$	$7n+1$	$7n+2$	$7n+4$	
8	$8n$	$8n+1$	$8n+4$		
9	$9n$	$9n+1$	$9n+4$	$9n+7$	
10	$10n$	$10n\pm 1$	$10n\pm 4$	$10n\pm 5$	
11	$11n$	$11n+1$	$11n+3$	$11n+4$	$11n+5$
		$11n+9$			
12	$12n$	$12n+1$	$12n+4$	$12n+9$	
13	$13n$	$13n\pm 1$	$13n\pm 3$	$13n\pm 4$	
14	$14n$	$14n+1$	$14n+2$	$14n+4$	$14n+7$
		$14n+8$	$14n+9$	$14n+11$	
15	$15n$	$15n+1$	$15n+4$	$15n+6$	$15n+9$
		$15n+10$			
16	$16n$	$16n+1$	$16n+4$	$16n+9$	
17	$17n$	$17n\pm 1$	$17n\pm 2$	$17n\pm 4$	$17n\pm 8$
18	$18n$	$18n+1$	$18n+4$	$18n+7$	$18n+10$
		$18n+13$	$18n+16$		
19	$19n$	$19n+1$	$19n+4$	$19n+5$	$19n+6$
		$19n+7$	$19n+9$	$19n+11$	$19n+16$
		$19n+17$			
20	$20n$	$20n+1$	$20n+4$	$20n+5$	$20n+9$
		$20n+16$			

46. *Scholium* 2. Hence, by way of exclusion, arises the following table, which exhibits all those forms, referred to the same moduli, that can never become squares, and by means of which we may frequently ascertain whether a given number be a square or not, without absolutely performing the extraction.

Table of impossible Forms for Square Numbers for every Modulus, from 2 to 20.

Moduli.	*Impossible Formulæ.*				
3	$3n+2$				
4	$4n+2$	$4n+3$			
5	$5n+2$	$5n+3$			
6	$6n+2$	$6n+5$			
7	$7n+3$	$7n+5$	$7n+6$		
8	$8n\pm2$	$8n\pm3$	$8n+7$		
9	$9n+2$	$9n\pm3$	$9n+5$	$9n+8$	
10	$10n\pm2$	$10n\pm3$			
11	$11n+2$	$11n+6$	$11n+7$	$11n+8$	$11n+10$
12	$12n\pm2$	$12n+3$	$12n\pm5$	$12n+6$	$12n+8$
		$12n+10$			
13	$13n\pm2$	$13n\pm5$	$13n\pm6$		
14	$14n+3$	$14n+5$	$14n+6$	$14n+10$	$14n+12$
		$14n+13$			
15	$15n+2$	$15n+3$	$15n+5$	$15n+7$	$15n+8$
		$15n+11$	$15n+12$	$15n+13$	$15n+14$
16	$16n\pm2$	$16n\pm3$	$16n\pm5$	$16n\pm6$	$16n+7$
		$16n+8$	$16n+12$	$16n+15$	
17	$17n\pm3$	$17n\pm5$	$17n\pm6$	$17n\pm7$	
18	$18n+2$	$18n\pm3$	$18n+5$	$18n\pm6$	$18n+8$
		$18n+9$	$18n+11$	$18n+14$	$18n+17$
19	$19n+2$	$19n+3$	$19n+8$	$19n+10$	$19n+12$
		$19n+13$	$19n+14$	$19n+15$	$19n+18$
20	$20n\pm2$	$20n\pm3$	$20n\pm6$	$20n\pm7$	$20n\pm8$
		$20n+10$	$20n+11$	$20n+15$	$20n+19$

Lemma.

47. In order to simplify and abridge the demonstration in the following propositions, it will be proper to make a few general observations on equations of the form $at^2 + bu^2 = w^2$.

And, first, we may always consider a and b as quantities that have no square factor, or divisor; for, if $a = a'\phi^2$, and $b = b'\theta^2$, our equation becomes $a'\phi^2 t^2 \pm b\theta^2 u^2 = w^2$; or, making $\phi t = t'$, and $\theta u = u'$, we have $a't'^2 \pm b'u'^2 = w^2$; and, consequently, if the above equation obtain when the quantities a and b, or either of them, have a square divisor, it may always be put in another form, $a't'^2 \pm b'u'^2 = w^2$, in which the similar quantities a' and b' have not a square divisor; and, therefore, in what follows, with regard to the possibility or impossibility of equations of the form $at^2 \pm bu^2$, we may always consider a and b as not having a square divisor.

Again, if the equation $at^2 \pm bu^2 = w^2$ be possible, when t^2, u^2, and w^2, have a common square divisor ϕ^2, it is also possible when divided by it; thus, if

$a\phi^2 t'^2 \pm b\phi^2 u'^2 = \phi^2 w'^2$ be possible, so also is

$$at'^2 \pm bu'^2 = w'^2,$$

which is a similar equation to the first, and in which t'^2, u'^2, and w'^2, have now no common square divisor. And it is evident, that no two of these squares can have a common divisor, unless the third square has the same. For, if it be possible, let $t^2 = t'^2\phi^2$, and $u^2 = u'^2\phi^2$; then, $at'^2\phi^2 \pm bu'^2\phi^2 = w^2$, where the first side of the equation is divisible by ϕ^2, but the second is not, by the supposition, and yet it is equal to the first, which is absurd: and the same

may be demonstrated if any other two of those squares are supposed to contain a square divisor, not common with the third; a and b having no square divisor, as is shown above.

Hence, then, we may draw this conclusion, in any case where we are investigating the possibility of an equation, of the form $at^2 \pm bu^2 = w^2$, the quantities a and b may be considered as not containing a square divisor; and also the three quantities t, u, and w, as being prime to each other: for if the equation be possible under these conditions, it is possible when those quantities have a common measure; and if it be impossible under the former case, it is also impossible under the latter.

And it may be farther observed, that if any equation of the form $at^2 \pm bu^2 = w^2$ be impossible in integers, it is so likewise in fractions; for make

$t = \frac{r}{s}$, $u = \frac{y}{v}$, and $w = \frac{x}{z}$, then it becomes

$a\frac{r^2}{s^2} \pm u\frac{y^2}{v^2} = \frac{x^2}{z^2}$; which reduces it to this,

$ar^2v^2 \pm bs^2y^2 = \frac{s^2v^2x^2}{z^2}$; or, making

$r^2v^2 = t^2$, $s^2y^2 = u^2$, and $\frac{s^2v^2x^2}{z^2} = w^2$,

which last must evidently be an integral square, we have again $at^2 \pm bu^2 = w^2$; so that the possibility of any fractional equation of this kind depends upon a similar integral équation, and if, therefore, an equation be impossible, in integers, with any specified value of a and b, it is also impossible in fractions.

Cor. The same that has been proved of the equation $at^2 \pm bu^2 = w^2$ is also true of the equation $at^3 \pm bu^3 = w^3$, and, generally, of the equation $at^n \pm bu^n = w^n$; it being always understood, that neither a nor b contain any factor that is ~~not~~ a complete *nth* power.

PROP. IV.

48. The equation $2t^2 \pm 3qu^2 = w^2$ is always impossible, either in integers or fractions, if q be taken prime to 3.

We have seen, in the foregoing *lemma*, that it will be sufficient to consider t and u as integers; and that we may always suppose t^2, u^2, and w^2, to be prime to each other. Now, since $3qu^2$ is always of the form $3n$, whatever may be the form of u^2; and since t^2 must be of one of the forms $3n$, or $3n+1$ (art. 45), we shall have, either,

$$\text{1st,} \quad (3p+2)3n \pm 3qu^2 = w^2; \text{ or}$$
$$\text{2d,} \quad (3p+2)(3n+1) \pm 3qu^2 = w^2.$$

But in the first equation, where we suppose $t^2 \doteq 3n$, we have the first side of the equation divisible by 3; and, consequently, the other side w^2, is also divisible by 3; that is, both t^2 and w^2 are of the form $3n$; whereas we have seen that they are prime to each other, which is absurd; therefore, the equation is impossible, when t is of the form $3n$.

Again, in the second equation, in which we have supposed $t^2 \doteq 3n+1$, we have

$$(3p+2) \times (3n+1) \pm 3qu^2 = w^2, \text{ or}$$
$$9pn + 6n + 3p + 2 \pm 3qu^2 = w^2, \text{ or}$$
$$3(3pn + 2n + p \pm qu^2) + 2 = w^2; \text{ that is,}$$
$$w^2 \doteq 3n' + 2,$$

which is impossible (art. 46); therefore, the equation is always impossible, under the above limitation of q. — Q. E. D.

Remark. If q had not been taken under the above restriction, our demonstration would necessarily have failed; because, in that case, if we put $q = 3q'$, we should have had $3qu^2 = q' . 9u^2$; or, making $9u^2 = u'^2$, $3qu^2 = q'u'^2$; which would evidently have altered the form of the equation. But, under the above restriction, we are led to several impossible cases, by taking $p = o$, or an integer number, and q any number not divisible by 3: thus

$$\begin{array}{lll} p = 0, \text{ then} & 2t^2 \pm 3u^2 = w^2; \\ p = 1, \text{ then} & 5t^2 \pm 3u^2 = w^2; \\ p = 2, \text{ then} & 8t^2 \pm 3u^2 = w^2; \\ \&c. & \&c. & \&c. \end{array}$$

are all impossible equations, which may be carried on at pleasure.

In the above, we have taken $q = 1$; but if $q = 2$ and

$$\begin{array}{lll} p = 0, \text{ then} & 2t^2 \pm 6u^2 = w^2; \\ p = 1, \text{ then} & 5t^2 \pm 6u^2 = w^2; \\ p = 2, \text{ then} & 8t^2 \pm 6u^2 = w^2; \\ \&c. & \&c. & \&c. \end{array}$$

are also impossible equations; and thus we may proceed to find impossible equations, to any length, at pleasure.

PROP. V.

49. The equation $(5p \pm 2)t^2 \mp 5qu^2 = w^2$ is impossible, when q is prime to 5.

For t^2 must be of one of the three forms, $5n$, $5n + 1$, $5n - 1$; which furnish the three following equations:

$$1\text{st}, \ (5p \pm 2) \times 5n \mp 5qu^2 = w^2;$$
$$2\text{d}, \ (5p \pm 2) \times (5n+1) \mp 5qu^2 = w^2;$$
$$3\text{d}, \ (5p \pm 2) \times (5n-1) \mp 5qu^2 = w^2.$$

In the first equation, in which we suppose $t^2 \doteqdot 5n$, we have evidently $w^2 \doteqdot 5n'$ also; that is, t^2 and w^2 are both divisible by 5, whereas, by the preceding *lemma*, they are prime to each other, which is absurd; therefore, the equation is impossible, when $t^2 \doteqdot 5n$.

In the second equation, in which we suppose

$t^2 \doteqdot 5n+1$, we have
$$(5p \pm 2) \times (5n+1) \mp 5qu^2 = w^2, \text{ or}$$
$$25pn \pm 10n + 5p \pm 2 \mp 5qu^2 = w^2, \text{ or}$$
$$5(5pn \pm 2n + p \mp qu^2) \pm 2 = w^2;$$

that is, $w^2 \doteqdot 5n \pm 2$, which is impossible (cor. 2, art. 43).

In the third equation, we suppose

$t^2 \doteqdot 5n-1$, which gives
$$(5p \pm 2) \times (5n-1) \mp 5qu^2 = w^2, \text{ or}$$
$$25pn \pm 10n - 5p \mp 2 \mp 5qu^2 = w^2, \text{ or}$$
$$5(5pn \pm 2n - p \mp qu^2) \mp 2 = w^2;$$

that is, $w^2 \doteqdot 5n \mp 2$, which is also impossible; and, consequently, as t^2 must be of one of those forms, it follows, that the equation $(5p \pm 2)t^2 \mp 5qu^2 = w^2$ is always impossible, when q is prime to 5.

Cor. By means of this proposition, we arrive at the following set of impossible forms to modulus 5, which may be carried to any length.

$2t^2 \mp 5u^2 = w^2$,	$2t^2 \mp 10u^2 = w^2$,
$3t^2 \mp 5u^2 = w^2$,	$3t^2 \mp 10u^2 = w^2$,
$7t^2 \mp 5u^2 = w^2$,	$7t^2 \mp 10u^2 = w^2$,
$8t^2 \mp 5u^2 = w^2$,	$8t^2 \mp 10u^2 = w^2$,
&c. &c. &c.	&c. &c. &c.

PROP. VI.

50. Every equation that falls under any of the following forms is impossible; *viz.*

$$(7p+3)t^2 \pm 7qu^2 = w^2,$$
$$(7p+5)t^2 \pm 7qu^2 = w^2,$$
$$(7p+6)t^2 \pm 7qu^2 = w^2,$$

it being always understood that q is not divisible by 7.

For every square number is of one of the forms $7n$, $7n+1$, $7n+2$, or $7n+4$ (art. 45).

But t^2 cannot be of the form $7n$, in any of the equations, because then w^2 would be of the same form; that is, both t^2 and w^2 would be divisible by 7, which is contrary to the supposition, since they are prime to each other; therefore, t^2 must be of one of the other forms, if there be any case in which these equations are possible.

Now in the first equation, if we suppose $t^2 \doteqdot 7n+1$, we have

$$(7p+3)\times(7n+1) \pm 7qu^2 = w^2, \text{ or}$$
$$49pn+21n+7p+3 \pm 7qu^2 = w^2, \text{ or}$$
$$7(7pn+3n+p \pm qu^2)+3 = w^2, \text{ or}$$
$$w^2 \doteqdot 7n'+3;$$

an impossible form for squares (art. 46).

Again, suppose $t^2 \doteqdot 7n+2$; then

$$(7p+3)\times(7n+2) \pm 7qu^2 = w^2, \text{ or}$$
$$49pn+21n+14p+6 \pm 7qu^2 = w^2, \text{ or}$$
$$7(7pn+3n+2p \pm qu^2)+6 = w^2, \text{ or}$$
$$w^2 \doteqdot 7n+6;$$

an impossible form, by the same article.

If $t^2 \doteqdot 7n+4$, we have

$$(7p+3)\times(7n+4)\pm 7qu^2 = w^2, \text{ or}$$
$$49pn+21n+28p+12\pm 7qu^2 = w^2, \text{ or}$$
$$7(7pn+3n+4p+qu^2)+12 = w^2, \text{ or}$$
$$w^2 \doteqdot 7n+5;$$

an impossible form.

Therefore, the first equation is impossible under every form of t^2, q being prime to 7.

In the second equation,

$$(7p+5)t^2 \pm 7qu^2 = w^2,$$

by assuming t^2 successively of the three forms $7n+1$, $7n+2$, $7n+3$, we are led to the following results.

$t^2 \doteqdot 7n+1$, then $\left\{ (7p+5)\times(7n+1)\pm 7qu^2 = w^2 \doteqdot 7n'+5; \right.$

$t^2 \doteqdot 7n+2$, then $\left\{ (7p+5)\times(7n+2)\pm 7qu^2 = w^2 \doteqdot 7n'+3; \right.$

$t^2 \doteqdot 7n+4$, then $\left\{ (7p+5)\times(7n+4)\pm 7qu^2 = w^2 \doteqdot 7n'+6; \right.$

all of which are impossible forms: and, consequently, the second equation,

$$(7p+5)t^2 \pm 7qu^2 = w^2,$$

is always impossible, q being prime to 7.

In the third equation,

$$(7p+6)t^2 \pm 7qu^2 = w^2,$$

by assuming, as before, t^2 of the forms $7n+1$, $7n+2$, $7n+3$, we have

$t^2 \doteqdot 7n+1$, then $\left\{ \begin{array}{l} (7p+6)\times(7n+1)\pm 7qu^2 = w^2 \doteqdot \\ \qquad 7n'+6; \end{array} \right.$

$t^2 \doteqdot 7n+2$, then $\left\{ \begin{array}{l} (7p+6)\times(7n+2)\pm 7qu^2 = w^2 \doteqdot \\ \qquad 7n'+5; \end{array} \right.$

$t^2 \doteqdot 7n+4$, then $\left\{ \begin{array}{l} (7p+6)\times(7n+4)\pm 7qu^2 = w^2 \doteqdot \\ \qquad 7n'+3; \end{array} \right.$

which are likewise impossible forms: and, consequently, the three given equations are all impossible, when q is prime to 7. — Q. E. D.

Cor. This proposition furnishes us with the following particular cases, which, like the foregoing, may be extended to any length.

$3t^2 \pm 7u^2 = w^2$,	$3t^2 \pm 14u^2 = w^2$,
$5t^2 \pm 7u^2 = w^2$,	$5t^2 \pm 14u^2 = w^2$,
$6t^2 \pm 7u^2 = w^2$,	$6t^2 \pm 14u^2 = w^2$,
$10t^2 \pm 7u^2 = w^2$,	$10t^2 \pm 14u^2 = w^2$,
$12t^2 \pm 7u^2 = w^2$,	$12t^2 \pm 14u^2 = w^2$,
$13t^2 \pm 7u^2 = w^2$,	$13t^2 \pm 14u^2 = w^2$,
&c. &c. &c.	&c. &c. &c.

Scholium. If we examine the impossible forms of the foregoing propositions, it will be readily observed, that the multipliers of t^2 are all impossible forms, with regard to that particular prime modulus to which they are referred: thus,

$3p+2$, to modulus 3;

$5p\pm 2$, to modulus 5;

$\left.\begin{array}{l} 7p+3, \\ 7p+5, \\ 7p+6, \end{array}\right\}$ to modulus 7.

And hence we are led to an inference, that the same is true for any other prime modulus; that is, the

Equations

$$(11p+2)t^2 \pm 11qu^2 = w^2,$$
$$(11p+6)t^2 \pm 11qu^2 = w^2,$$
$$(11p+7)t^2 \pm 11qu^2 = w^2,$$
$$(11p+8)t^2 \pm 11qu^2 = w^2,$$
$$(11p+10)t^2 \pm 11qu^2 = w^2,$$

are all impossible, while q is taken prime to 11.

Also,

$$(13p \pm 2)t^2 \mp 13qu^2 = w^2,$$
$$(13p \pm 5)t^2 \mp 13qu^2 = w^2,$$
$$(13p \pm 6)t^2 \mp 13qu^2 = w^2,$$

when q is taken prime to the modulus 13;

And

$$(17p \pm 3)t^2 \mp 17qu^2 = w^2,$$
$$(17p \pm 5)t^2 \mp 17qu^2 = w^2,$$
$$(17p \pm 6)t^2 \mp 17qu^2 = w^2,$$
$$(17p \pm 7)t^2 \mp 17qu^2 = w^2,$$

when q is taken prime to the modulus 17;

Likewise,

$$(19p+2)t^2 \pm 19qu^2 = w^2,$$
$$(19p+3)t^2 \pm 19qu^2 = w^2,$$
$$(19p+8)t^2 \pm 19qu^2 = w^2,$$
$$(19p+10)t^2 \pm 19qu^2 = w^2,$$
$$(19p+12)t^2 \pm 19qu^2 = w^2,$$
$$(19p+13)t^2 \pm 19qu^2 = w^2,$$
$$(19p+14)t^2 \pm 19qu^2 = w^2,$$
$$(19p+15)t^2 \pm 19qu^2 = w^2,$$
$$(19p+18)t^2 \pm 19qu^2 = w^2,$$

when q is prime to 19; are all impossible forms of equations in rational numbers.

These latter forms are only deduced from observation, upon the supposition that the product of

a possible and impossible form is also of an impossible form; which property is, however, rigorously demonstrated in the two following propositions.

With regard to such moduli as are not prime numbers, they are evidently reducible to others that are prime, by means of the indeterminate letter q.

PROP. VII.

51. Let a be a prime number, and ϕ any number prime to a; then, if the series of square numbers,

$$\phi^2,\ 2^2\phi^2,\ 3^2\phi^2,\ 4^2\phi^2,\ \&c.,\ \cdots \left(\frac{a-1}{2}\right)^2\phi^2,$$

be divided by a, they will each leave a different positive remainder.

For if it be possible, that any two of these squares, when divided by a, can leave the same remainder, let them be represented by $m^2\phi^2$, and $n^2\phi^2$; that is, let $m^2\phi^2 = ap + r$, and $n^2\phi^2 = aq + r$, r being the common remainder of each; then, it is evident, that the difference of those squares,

$$m^2\phi^2 - n^2\phi^2 = (ap + r) - (aq + r) = ap - aq,$$

will be divisible by a; but this is impossible, for

$$m^2\phi^2 - n^2\phi^2 = \phi^2 \times (m + n) \times (m - n);$$

and since both m and n are less than $\frac{1}{2}a$, their sum $(m + n) < a$, and, consequently, prime to it, because a is a prime number, and the same is evidently true of the factor $(m - n)$; also ϕ^2 is prime to a, by the hypothesis; and, therefore, the three factors, ϕ^2, $(m + n)$, and $(m - n)$, are each prime to a; and, consequently, their product $\phi^2(m^2 - n^2)$ is so likewise (cor. 1, art. 11): hence, then, the squares $m^2\phi^2$,

and $n^2\phi^2$, cannot be of the forms $pa+r$, and $qa+r$; that is, they cannot have the same common remainder. Since, therefore, no two of those squares, to modulus a, can have a common remainder, these remainders are all different from each other.

Q. E. D.

Cor. 1. The same is also true of the negative remainders, of the same series, to the same modulus, by taking the quotient in excess; that is, if the series of squares,

$$\phi^2,\ 2^2\phi^2,\ 3^2\phi^2,\ 4^2\phi^2,\ ---\ \left(\frac{a-1}{2}\right)^2\phi^2,$$

be divided by a, and the quotient be taken in excess, so that the remainders may become negative; then will these negative remainders be all different from each other. The demonstration of which is exactly the same as that of the foregoing proposition, by making $m^2\phi^2 = pa-r$, and $n^2\phi^2 = qa-r$; $-r$ being supposed the common negative remainder.

Cor. 2. Since, in the above demonstration, it is only necessary that ϕ^2 should be prime to a, therefore, all that has been proved of the series of squares,

$$\phi^2,\ 2^2\phi^2,\ 3^2\phi^2,\ 4^2\phi^2,\ ---\ \left(\frac{a-1}{2}\right)^2\phi^2,$$

is equally true of any other series of squares,

$$\pi^2,\ 2^2\pi^2,\ 3^2\pi^2,\ 4^2\pi^2,\ ---\ \left(\frac{a-1}{2}\right)^2\pi^2,$$

providing π^2 be prime to a; and the remainder of this last series will be exactly the same as the remainders in the former series, except that their order may be changed. For it has been de-

monstrated (art. 44), that the forms of all square numbers, to any modulus a, are the same as those of the squares

$$1^2,\ 2^2,\ 3^2,\ 4^2,\ \&c.,\ - - - \left(\frac{a-1}{2}\right)^2;$$

the number of forms are, therefore, limited never to exceed $\frac{a-1}{2}$; and, consequently, the same remainders will recur in any series, and only the order of them will be changed: and hence it follows, that, whatever remainder any square ϕ^2 may leave, another square $m^2\pi^2$ may be found, that will leave the same remainder; and, therefore, if $sm^2 - \phi^2$ be divisible by a, then $sm^2 - m^2\pi^2 = m^2 \times (s - \pi^2)$ is also divisible by a, and likewise $s - \pi^2$, because m^2 is supposed prime to a.

PROP. VIII.

52. The multiplication of a possible and impossible form of square numbers, to the same modulus, always produces an impossible form.

Let a be any prime number, and let

$$r_1,\ r_2,\ r_3,\ r_4,\ \&c.,$$

be the remainders arising from dividing the series of squares,

$$\phi^2,\ 2^2\phi^2,\ 3^2\phi^2,\ 4^2\phi^2,\ \&c.,\ \left(\frac{a-1}{2}\right)^2\phi^2,$$

by the modulus a, then will

$$ap + r_1,\ ap + r_2,\ ap + r_3,\ \&c.,$$

represent all the possible forms of square numbers, to modulus a (art. 44); and, since the number of

these remainders r_1, r_2, r_3, &c., never exceeds $\frac{a-1}{2}$, it follows, that there are the same number of impossible forms; which may be represented by

$$aq+s_1,\ aq+s_2,\ aq+s_3,\ \&c.;$$

and it is to be demonstrated, that any one of these impossible forms, being multiplied by any of the above possible forms, will produce an impossible form.

For let $m^2\phi^2 = ap + r_m$ represent any possible form, and $aq+s_n$ any one of the impossible forms; then, if $(ap+r_m)\times(aq+s_n)$ produce a possible form, $m^2\phi^2\times(aq+s_n) = aqm^2\phi^2 + s_nm^2\phi^2$ will be the same; or, $s_nm^2\phi^2$, because the first part $aqm^2\phi^2$ is divisible by a; but if this be a possible form, that is, if, when divided by a, the remainder be found in the series of possible remainders,

$$r_1,\ r_2,\ r_3,\ r_4,\ \&c.,$$

let it be represented by r_v, then it is evident, that the square $v^2\phi^2$, whence this remainder is derived, being of the form $ap+r_v$, and $s_nm^2\phi^2$ being supposed also of the form $ap'+r_v$, we should have

$$s_nm^2\phi^2 - v^2\phi^2 = (ap'+r_v) - (ap+r_v) =$$
$$(ap'-ap) \text{ divisible by } a;$$

and, consequently,

$$(s_nm^2\phi^2 - v^2\phi^2) = \phi^2(s_nm^2 - v^2) \text{ divisible by } a;$$

but ϕ^2 is prime to a, therefore it must be

$$(s_nm^2 - v^2) \div a.$$

But, whatever remainder the square v^2 may give to modulus a, another square, $m^2\pi^2$, may be found, that will have the same remainder (cor. 2, art. 51); and, consequently, if $(s_nm^2 - v^2)$ be $\div a$, then will

$(s_n m^2 - m^2\pi^2)$ be $\div a$; but $(s_n m^2 - m^2\pi^2) = m^2(s_n - \pi^2)$, and m is less than a, and, therefore, prime to it; consequently, if $m^2(s_n - \pi^2)$ be divisible by a, $(s_n - \pi^2)$ must be so likewise; that is, π^2 divided by a must have a remainder s_n, or $\pi^2 \doteq ap + s_n$; but this is an impossible form of squares by the hypothesis, therefore, $(s_n - \pi^2)$ is not divisible by a; that is, the product $(ap + r_m) \times (aq + s_n)$ cannot, when divided by a, leave for a remainder any number in the series of possible remainders,

$$r_1, \ r_2, \ r_3, \ r_4, \ \&c.;$$

and, therefore, the remainder of this product must fall in the other series

$$s_1, \ s_2, \ s_3, \ s_4, \ \&c.;$$

and, consequently, $(ap + r_m) \times (aq + s_n)$ is always an impossible form; that is, the product arising from a possible and impossible form, is itself also an impossible form. — Q. E. D.

Hence we have demonstrated the truth of what was deduced from observation in the *scholium* (art. 50).

PROP. IX.

53. To ascertain the possibility or impossibility of every equation of the form

$$ax^2 + by^2 = cz^2.$$

The rule for this purpose is deduced immediately from the foregoing proposition; *viz.* that a possible form multiplied by an impossible form always produces the latter: for from hence it follows, that ax^2 is always of the same form as a, with regard to possible or impossible; and, in the same manner, by^2

is of the same form as b, and cz^2 of the same form as c. Now $ax^2 = na$, therefore $cz^2 - by^2$ must be also of the form na; and, consequently, cz^2 must leave the same remainder, when divided by a, as by^2 does when divided by the same: it is evident, therefore, that these remainders must be both of the class of possible remainders, or both impossible, for otherwise they could not be equal; but these remainders will be of the same classes as c and b are; and hence it follows, that, if c and b are both found among the remainders to modulus a, or neither of them are found there, the equation may be possible, but if one of them is found there, and the other not, the equation is certainly impossible. And, in the same manner, if a and c be both found among the remainders to modulus b, or if neither of them be found there, the equation may be possible; but if one is found there, and the other not, the equation is certainly impossible. And, for the same reason, a and $-b$, or, which is equivalent, a and $c-b$, must be either both found among the remainders of modulus c, or neither of them, if the equation be possible. Having thus shown the principle of the rule, it may be delivered more briefly thus:

Find the forms of all squares to modulus a, or, which is the same, the remainders arising from dividing the squares,

$$1^2,\ 2^2,\ 3^2,\ 4^2,\ \&c.,\ (\tfrac{1}{2}a)^2, \text{ by } a;$$

and, if b and c are both found in this series of remainders, or if neither of them be found there, the equation may obtain; but if one of them be found there, and the other not, the equation is certainly

impossible, and it will be needless to proceed any farther in the investigation. But if one of the two first conditions have place, then find the remainders of

$$1^2,\ 2^2,\ 3^2,\ 4^2,\ \&c.,\ (\tfrac{1}{2}b)^2, \text{ divided by } b;$$

and these remainders must be submitted to the same test, with regard to a and c; and if one of them be found there, and the other not, the equation is impossible, and we need proceed no farther in the investigation. But if this be not the case, find the remainders of

$$1^2,\ 2^2,\ 3^2,\ 4^2,\ \&c.,\ (\tfrac{1}{2}c)^2, \text{ divided by } c;$$

and if a and $(c-b)$ be both found in this series, or if neither of them be found there, the equation is possible, supposing the same to have had place in the other two series; but otherwise the equation is certainly impossible.

It is to be observed, that, when any one of those three quantities is greater than the modulus, with the remainders of which it is compared, it must be divided by the modulus and remainder used, instead of the quantity itself. It may be also farther observed, that, if any one of the three quantities, a, b, or c, be unity, only two trials will be necessary, and, if two of them be unity, but one.

These operations will be considerably abridged by means of the following table, which exhibits the remainders to every modulus, from 2 to 51, excepting only those numbers that contain square factors, because a, b, and c, contain no square factors (by art. 47); and hence the possibility or impossibility of any equation, in which the coefficients do not exceed 50, may be ascertained by inspection.

Table of the Remainders of Squares to every Modulus, from 2 to 51.

Moduli.	Remainders.														
2	1														
3	1														
5	1	4													
6	1	3	4												
7	1	2	4												
10	1	4	5	6	9										
11	1	3	4	5	9										
13	1	3	4	9	10	12									
14	1	2	4	7	8	9	11								
15	1	4	6	9	10										
17	1	2	4	8	9	13	15	16							
19	1	4	5	6	7	9	11	16	17						
21	1	4	7	9	15	16	18								
22	1	3	4	7	9	11	12	14	15	16	20				
23	1	2	3	4	6	8	9	12	13	16	18				
26	1	3	4	9	10	12	14	16	17	22	23	25			
29	1	4	5	6	7	9	13	16	20	22	23	24	25	28	
30	1	4	6	9	10	15	16	19	21	24	25				
31	1	2	4	5	7	8	9	10	14	16	18	19	20	25	28
33	1	3	4	9	12	15	16	22	25	27	31				
34	1	2	4	8	9	13	15	16	17	18	19	21	25	26	30
		32	33												
35	1	4	9	11	14	15	16	21	25	29	30				
37	1	3	4	7	9	10	11	12	16	21	25	26	27	28	30
		33	34	36											
38	1	4	5	6	7	9	11	16	17	19	20	23	24	25	26
		28	30	35	36										
39	1	3	4	9	10	12	13	16	22	25	27	30	36		
41	1	2	4	5	8	9	10	16	18	20	21	23	25	31	32
		33	36	37	39	40									
42	1	4	7	9	15	16	18	21	22	25	28	30	36	37	39
43	1	4	6	9	10	11	13	14	15	16	17	21	23	24	25
		31	35	36	38	40	41								
46	1	2	3	4	6	8	9	12	13	16	18	23	24	25	26
		27	29	31	32	35	36	39	41						
47	1	2	3	4	6	7	8	9	12	14	16	17	18	21	24
		25	27	28	32	34	36	37	42						
51	1	4	9	13	15	16	18	19	21	23	25	30	34	36	42
		43	49												

Ex. 1. It is required to ascertain, whether the equation $7x^2+11y^2=13z^2$ be possible or impossible.

$$11 \doteqdot 7n+4, \text{ and } 13 \doteqdot 7n+6.$$

Now 4 is found in the table to belong to modulus 7, but 6 is not found there, whence the equation is impossible.

Ex. 2. Find whether the equation

$7x^2+11y^2=23z^2$ be possible or impossible.

$$11 \doteqdot 7n+4, \text{ and } 23 \doteqdot 7n+2.$$

And 4 and 2 being both found to belong to modulus 7, the equation may be possible.

Again,

$$7 \doteqdot 11n+7, \text{ and } 23 \doteqdot 11n+1.$$

Now one of these remainders, 1, belongs to modulus 11, but 7 does not, therefore the equation is impossible.

Ex. 3. Find whether the equation

$14x^2+6y^2=17z^2$ be possible or impossible.

$$6 \doteqdot 14n+6,\ 17 \doteqdot 14n+3.$$

And neither 6 nor 3 belongs to modulus 14, therefore the equation may be possible.

Again,

$$14 \doteqdot 6n+2,\ 17 \doteqdot 6n+5.$$

And neither 2 nor 5 belongs to modulus 6, the equation, therefore, may still be possible.

Also,

$$14 \doteqdot 7n+14, \text{ and } 17-6 \doteqdot 17n+11.$$

And neither 11 nor 14 belongs to modulus 17, therefore the equation is possible. In fact,

$$14 \cdot 11^2+6 \cdot 1^2=17 \cdot 10^2.$$

These examples will be quite sufficient for ex-

plaining our operation; it may not, however, be superfluous to add, that, when an equation appears under the form $ax^2 - by^2 = cz^2$, it is immediately transformed to the sort of equation we have been investigating, by writing it $cz^2 + by^2 = ax^2$. The cases, in which one or two of the coefficients become unity, are evidently involved in the general form above given, and, therefore, need no examples *.

PROP. X.

54. The equation $x^2 - y^2 = az^2$ is always possible in integers.

For, if we resolve $x^2 - y^2$ into its factors $x + y$, and $x - y$ (which are the only two literal factors that the formula admits of), and also az^2 into any two factors amt^2, and mu^2, we have, by comparison,

$$\left.\begin{array}{l} x+y=amt^2, \\ x-y=mu^2, \end{array}\right\} \text{ or } \left\{\begin{array}{l} x+y=mu^2, \\ x-y=amt^2, \end{array}\right.$$

which, by multiplication, becomes $x^2 - y^2 = am^2t^2u^2$, or $x^2 - y^2 = az^2$, by making $z = mtu$.

Now these equations give,

$$\text{1st, } x = \frac{amt^2 + mu^2}{2}, \text{ and } y = \frac{amt^2 - mu^2}{2};$$

$$\text{2d, } x = \frac{mu^2 + amt^2}{2}, \text{ and } y = \frac{mu^2 - amt^2}{2}.$$

On making $m = 2$, in order to clear the expressions of fractions, they become,

$$\text{1st, } x = at^2 + u^2, \text{ and } y = at^2 - u^2;$$
$$\text{2d, } x = u^2 + at^2, \text{ and } y = u^2 - at^2:$$

therefore, the equation is always possible in integers. — Q. E. D.

* See PART II. chap. iii. prop. 5.

We may also take $m=1$, or any odd number, only observing, that if a be odd, we must have t and u both odd; for, otherwise, x and y would not be integers. And if a be even, then u must be even likewise.

Cor. 1. If a be a prime number, the solution above given is the only one the equation admits of in integers, for $x+y$ and $x-y$ are the only literal factors of x^2-y^2; and amt^2 and mu^2 are the only factors of az^2, with regard to form; and, consequently, one of the two equalities must obtain; but the quantities t and u being indeterminate, they will furnish an infinite number of numerical solutions. But if a be a composite number, then the equation may have, beside the two solutions given above, as many different literal solutions as there are different ways of producing a by two factors; thus, if $a=bc$, we may have

$$\text{1st, } \left\{ \begin{array}{l} x+y=amt^2, \\ x-y=mu^2, \end{array} \right\} \text{ or } \left\{ \begin{array}{l} x+y=mu^2, \\ x-y=amt^2; \end{array} \right. \text{ and,}$$

$$\text{2d, } \left\{ \begin{array}{l} x+y=bmt^2, \\ x-y=cmu^2, \end{array} \right\} \text{ or } \left\{ \begin{array}{l} x+y=cmu^2, \\ x-y=bmt^2. \end{array} \right.$$

Cor. 2. The equation $x^2-y^2=az^2$ includes the two forms $x^2-az^2=y^2$, and $x^2+az^2=y^2$; for, by transposition, the first of these becomes $x^2-y^2=az^2$, and the latter $y^2-x^2=az^2$, which are evidently both of the same form.

Therefore, if it be required to make $x^2+az^2=y^2$ a square, we may have $x=at^2-u^2$, or $=u^2-at^2$, and $z=2tu$; whence $x^2+az^2=(at^2+u^2)^2$; or we may have $x=\dfrac{at^2-u^2}{2}$, and $z=tu$, which give

$$x^2 + az^2 = \left(\frac{at^2 + u^2}{2}\right)^2.$$

And to make $x^2 - az^2 = y^2$ a square, we may assume $x = at^2 + u^2$, and $z = 2tu$, which give

$$x^2 - az^2 = (at^2 - u^2)^2, \text{ or } = (u^2 - at^2)^2;$$

or we may take

$$x = \frac{at^2 + u^2}{2}, \text{ and } z = tu.$$

Cor. 3. But if $a = 1$, and the equation becomes $x^2 + z^2 = y^2$, then we may have indifferently $x = t^2 - u^2$, and $z = 2tu$, or $x = 2tu$, and $z = t^2 - u^2$, unless there be any thing in the nature of the equation that limits these forms: as, for example, if it be necessary that one of the quantities, x or z, be even; then it is obvious, that the even quantity must have the form $2tu$.

With regard to the equation $x^2 - z^2 = y^2$, it gives either $x = t^2 + u^2$, and $z = 2tu$, or $z = t^2 - u^2$, both of which values of z answer the required conditions of the equation.

Ex. Find the values of x, y, and z, in the equation $x^2 - y^2 = 30z^2$.

Here the following substitutions may be made,

1. $\begin{cases} x + y = mt^2, \\ x - y = 30mu^2, \end{cases}$ or $\begin{cases} x + y = 30mt^2, \\ x - y = mu^2. \end{cases}$

2. $\begin{cases} x + y = 3mt^2, \\ x - y = 10mu^2, \end{cases}$ or $\begin{cases} x + y = 10mt^2, \\ x - y = 3mu^2. \end{cases}$

3. $\begin{cases} x + y = 2mt^2, \\ x - y = 15mu^2, \end{cases}$ or $\begin{cases} x + y = 15mt^2, \\ x - y = 2mu^2. \end{cases}$

4. $\begin{cases} x + y = 5mt^2, \\ x - y = 6mu, \end{cases}$ or $\begin{cases} x + y = 6mt^2, \\ x - y = 5mu^2. \end{cases}$

And making, in each of these, $m = 2$, in order to

avoid fractions, we have the following general integral values of x and y:

$$1.\quad \begin{cases} x = t^2 + 30u^2, \\ y = t^2 - 30u^2, \end{cases} \text{or} \quad \begin{cases} x = 30t^2 + u^2, \\ y = 30t^2 - u^2. \end{cases}$$

$$2.\quad \begin{cases} x = 3t^2 + 10u^2, \\ y = 3t^2 - 10u^2, \end{cases} \text{or} \quad \begin{cases} x = 10t^2 + 3u^2, \\ y = 10t^2 - 3u^2. \end{cases}$$

$$3.\quad \begin{cases} x = 2t^2 + 15u^2, \\ y = 2t^2 - 15u^2, \end{cases} \text{or} \quad \begin{cases} x = 15t^2 + 2u^2, \\ y = 15t^2 - 2u^2. \end{cases}$$

$$4.\quad \begin{cases} x = 5t^2 + 6u^2, \\ y = 5t^2 - 6u^2, \end{cases} \text{or} \quad \begin{cases} x = 6t^2 + 5u^2, \\ y = 6t^2 - 5u^2. \end{cases}$$

In which formulæ, t and u may be any integer numbers whatever.

PROP. XI.

55. The two indeterminate equations,

$$x^2 + y^2 = z^2, \text{ and } x^2 - y^2 = w^2,$$

cannot both obtain, with the same values of x and y.

For, in the first place, x and y may be considered prime to each other (art. 47), and, therefore, x and y both odd, or one even and one odd; and we see, immediately, that it is y that must be even: for if $x^2 \doteqdot 4n+1$, and $y \doteqdot 4n+1$, then $x^2 + y^2 \doteqdot 4n+2$, which cannot be a square; and if $x^2 \doteqdot 4n$, and $y^2 \doteqdot 4n+1$, then $x^2 - y^2 \doteqdot 4n+3$, which is also an impossible form; therefore x is odd and y even.

Hence, then (cor. 3, art. 54), we must have,

$$1\text{st}, \begin{cases} x = r^2 - s^2, \\ y = 2rs. \end{cases} \quad \Bigg| \quad 2\text{d}, \begin{cases} x = t^2 + u^2, \\ y = 2tu. \end{cases}$$

Which furnish the following equations:

$$\begin{cases} r^2 - s^2 = t^2 + u^2, \\ rs = tu. \end{cases}$$

Now, in these equations, r is prime to s, and t prime to u; for otherwise, x and y would have a common measure, which is contrary to the supposition; and, farther, as $x=r^2-s^2$ is odd, one of these quantities, r or s, is even, and the other odd; and the same is also true of t and u, because $t^2+u^2=x$ is an odd number.

Again, since $\frac{rs}{t}=u$ is an integer, either r or s, or both, must contain the factors of t; for otherwise the quotient would not be an integer: we may, therefore, make $t=ab$, supposing a, b, to be its two factors, which may always be done, because, in the case of t being a prime, we have only to make one of these two factors equal to unity: and, since these factors are also contained in rs, we may write $r=ar'$, and $s=bs'$, whence $u=r's'$; and now, substituting these values for r, s, t, and u, the above equation becomes

$$a^2r'^2-b^2s'^2=a^2b^2+r'^2s'^2.$$

And here, since r is prime to s, and t to u; r', s', a, and b, are all prime among themselves, as is evident; for if we suppose any two of the quantities to have a common measure, as, for example, a and b, then, since a and b enter, either separately or connectedly, into three of the above quantities, the fourth, $r's'$, must have the same common measure, that is, $t=ab$, and $u=r's'$, would have a common measure, whereas we have seen that they are prime to each other; and, consequently, r', s', a, and b, are all prime to one another.

Now, by transposition, this equation becomes

$$a^2r'^2 - s'^2r'^2 = a^2b^2 + s'^2b^2, \text{ or}$$
$$(a^2 - s'^2)r'^2 = (a^2 + s'^2)b^2, \text{ or}$$
$$\frac{a^2 + s'^2}{a^2 - s'^2} = \frac{r'^2}{b^2}.$$

And here, since a^2 is prime to s'^2, $a^2 + s'^2$ is prime to $a^2 - s'^2$, or they have only the common measure 2 (art. 8); and we have, therefore, these two cases to consider separately. First, suppose $a^2 + s'^2$ and $a^2 - s'^2$ to be prime to each other, then the fraction $\frac{a^2 + s'^2}{a^2 - s'^2}$ is in its lowest terms, as is also $\frac{r'^2}{b^2}$, because r' is prime to b; and hence, the two fractions being equal to each other, and in their lowest terms, we must have, as resulting from the first supposition,

$$\begin{cases} a^2 + s'^2 = r'^2, \\ a^2 - s'^2 = b^2. \end{cases}$$

Again, let $a^2 + s'^2$ and $a^2 - s'^2$ have a common measure 2, then

$$\frac{\frac{1}{2}(a^2 + s'^2)}{\frac{1}{2}(a^2 - s'^2)} = \frac{a^2 + s'^2}{a^2 - s'^2} = \frac{r'^2}{b^2};$$

the first and last of which fractions are in their lowest terms, and, consequently,

$$\left.\begin{array}{l} \frac{1}{2}(a^2 + s'^2) = r'^2, \\ \frac{1}{2}(a^2 - s'^2) = b^2, \end{array}\right\} \text{ or } \begin{cases} a^2 + s'^2 = 2r'^2, \\ a^2 - s'^2 = 2b^2; \end{cases}$$

the last of which gives

$$\begin{cases} a^2 = r'^2 + b^2, \\ s'^2 = r'^2 - b^2. \end{cases}$$

Now these two results in both cases are exactly similar to the original equations, only here the quantities are much smaller than in that, at least r', s', and b, a, are less than y, because $y = r's'ab$.

Hence, then, it follows, that, if the equations

$$\begin{cases} x^2+y^2=z^2, \\ x^2-y^2=w^2, \end{cases}$$

were both possible, with the same values of x and y, it would also be possible to find similar equations,

$$\begin{cases} x'^2+y'^2=z'^2, \\ x'^2-y'^2=w'^2; \end{cases}$$

which would also be possible, and in which $y'<y$. And, in the same manner, if these last were possible, we might still find others,

$$\begin{cases} x''^2+y''^2=z''^2, \\ x''^2-y''^2=w''^2, \end{cases}$$

where $y''<y$, and so on of others, *ad infinitum.*

But it is impossible for a series of positive integers,

$$y^2,\ y'^2,\ y''^2,\ y'''^2,\ \&c.,$$

to go on decreasing to infinity, without becoming zero; in which case our equations are

$$\begin{cases} x^2=z^2, \\ x^2=w^2. \end{cases}$$

And, consequently, the two proposed equations can never obtain, with the same values of x and y, except when $y=o$; that is, the double equality

$$\begin{cases} x^2+y^2=z^2, \\ x^2-y^2=w^2, \end{cases}$$

is impossible. — Q. E. D.

Cor. 1. Hence, also, it appears, that the two equations,

$$\begin{cases} x^2+y^2=2z^2, \\ x^2-y^2=2u^2, \end{cases}$$

are impossible, with the same values of x and y, for these may be reduced to

$$\begin{cases} x'^2 = z^2 + z'^2, \\ y'^2 = z^2 - w^2; \end{cases}$$

and the two last being impossible, the former are impossible also.

Cor. 2. The two equations

$$\begin{cases} 2x^2 + y^2 = z^2, \\ 2x^2 - y^2 = w^2, \end{cases}$$

are both impossible, with the same values of x and y.

For we may consider x and y as prime to each other; and, therefore, both odd, or one even and one odd; but they cannot be both odd, for then

$$2x^2 + y^2 = 2(4n+1) + (4n'+1) \doteq 4n+3,$$

which cannot be a square. Neither can x be even and y odd, for then

$$2x^2 - y^2 = 2(4n) - (4n'+1) \doteq 4n+3,$$

which is an impossible form. And if y were even and x odd, then

$$2x^2 + y^2 = 2(4n+1) + 4n' \doteq 4n+2,$$

which is also impossible; and, therefore, the two given equations cannot both obtain.

Cor. 3. And this again shows the impossibility of the two equations

$$\begin{cases} x^2 + 2y^2 = 2z^2, \\ x^2 - 2y^2 = 2w^2; \end{cases}$$

for, by doubling these, we have

$$\begin{cases} 2x^2 + (2y)^2 = (2z)^2, \\ 2x^2 - (2y)^2 = (2w)^2; \end{cases}$$

which we have seen are impossible.

PROP. XII.

56. The two indeterminate equations,

$$\begin{cases} x^2+2y^2=z^2, \\ x^2-2y^2=w^2, \end{cases}$$

are impossible, with the same values of x and y.

As, in the foregoing proposition, we may consider x and y as numbers prime to each other, also, as in that, x must be odd and y even; and, therefore, we must have (cor. 3, art. 54),

$$\text{1st, } \left\{\begin{array}{l} x=r^2-2s^2, \\ y=\quad 2rs, \end{array}\right\} \text{ or } \left\{\begin{array}{l} x=2s^2-r^2, \\ y=\quad 2rs. \end{array}\right.$$

$$\text{2d, } \left\{\begin{array}{l} x=t^2+2u^2, \\ y=\quad 2tu. \end{array}\right\} \text{ Therefore,}$$

$$\left\{\begin{array}{l} r^2-2s^2=t^2+2u^2, \text{ or } 2s^2-r^2=t^2+2u^2, \\ \qquad rs = \quad tu; \end{array}\right.$$

and it is to be demonstrated, that these two equalities cannot obtain at the same time.

Now, for the same reason as in the foregoing proposition, r is prime to s, and t to u; also, as in that, we may make $r=ar'$, $s=bs'$, $t=ab$, and $u=r's'$; which four quantities are all prime to each other, for the same reason as in the foregoing proposition; and these values, being substituted for r, s, t, and u, give,

$$\text{1st, } r'^2a^2-2s'^2b^2=a^2b^2+2r'^2s'^2.$$
$$\text{2d, } 2s'^2b^2-r'^2a^2=a^2b^2+2r'^2s'^2:$$

which, by transposition, &c., become

$$r'^2(a^2-2s'^2)=b^2(a^2+2s'^2),$$
$$b^2(2s'^2-a^2)=r'^2(2s'^2+a^2);$$

and, by division,

$$1\text{st}, \ \frac{a^2+2s'^2}{a^2-2s'^2}=\frac{r'^2}{b^2}; \qquad 2\text{d}, \ \frac{2s'^2+a^2}{2s'^2-a^2}=\frac{b^2}{r'^2}.$$

Now, since s^2 is prime to a^2, the numerators of these two first fractions are prime to their respective denominators, or they have only the common measure 2; for if $a^2+2s'^2$, and $a^2-2s'^2$, have any common measure, their sum $2a^2$ will have the same; but $2a^2$, and a^2+2s^2, can have no other common measure than 2, and this can only be when a is even; for, if a^2 be odd, a^2+2s^2 is odd, and is, therefore, not divisible by 2; and, if a be even, s must be odd, because they are prime to each other: also in this case we may make $a=2a'$, whence our two expressions become

$$8a'^2, \text{ and } 4a'^2+2s'^2;$$

and, after dividing by 2, we have

$$4a'^2, \text{ and } 2a'^2+s'^2;$$

one of which is even and the other odd, and they are, therefore, in this state, prime to each other; because s' is prime to a'. There are, therefore, two cases to consider separately: first, when the numerators and denominators are prime to each other; and, secondly, when they have the common measure 2.

In the first case, we must have,

$$1\text{st}, \begin{cases} a^2+2s'^2=r'^2, \\ a^2-2s'^2=b'^2; \end{cases} \qquad 2\text{d}, \begin{cases} 2s'^2+a^2=b^2, \\ 2s'^2-a^2=r'^2. \end{cases}$$

The second supposition gives,

$$1\text{st}, \begin{cases} a^2+2s'^2=2r'^2, \\ a^2-2s'^2=2b^2; \end{cases} \qquad 2\text{d}, \begin{cases} 2s'^2+a^2=2b^2, \\ 2s'^2-a^2=2r'^2. \end{cases}$$

Now the second and third of these forms are im-

possible (corollaries 2 and 3 of the foregoing proposition); and the fourth, being doubled, is similar to the first, being

$$(2s')^2 + 2a^2 = (2b)^2,$$
$$(2s')^2 - 2a^2 = (2r')^2.$$

And, therefore, if the original equation,

$$\begin{cases} x^2 + 2y^2 = z^2, \\ x^2 - 2y^2 = w^2, \end{cases}$$

be possible, it is also possible to find a similar equation,

$$\left\{\begin{array}{l} a^2 + 2s'^2 = r'^2, \\ a^2 - 2s'^2 = b^2, \end{array}\right\} \text{ or } \left\{\begin{array}{l} x'^2 + 2y'^2 = z'^2, \\ x'^2 - 2y'^2 = w'^2, \end{array}\right.$$

in which s or $y' < y$; because $y = abrs$.

And, in the same manner, if this last were possible, we might find another still less,

$$\begin{cases} x''^2 + 2y''^2 = z''^2, \\ x''^2 - 2y''^2 = w''^2, \end{cases}$$

in which $y'' < y'$; and so on of others still less, *ad infinitum:* whence we conclude, the same as in the foregoing proposition, that the two given equations,

$$\begin{cases} x^2 + 2y^2 = z^2, \\ x^2 - 2y^2 = w^2, \end{cases}$$

are impossible, with the same values of x and y.

Q. E. D.

Cor. Hence again, the two equations,

$$\begin{cases} 2x^2 + y^2 = 2z^2, \\ 2x^2 - y^2 = 2w^2, \end{cases}$$

are impossible; for, if we multiply these by 2, they become

$$\begin{cases} (2x)^2 + 2y^2 = (2z)^2, \\ (2x)^2 - 2y^2 = (2w)^2; \end{cases}$$

and this being impossible, the first is so likewise.

Scholium. As, in the following propositions, we shall have occasion to refer to the several impossible cases demonstrated in the two foregoing articles and their corollaries, it will not be amiss to collect them together under one point of view, as follows; *viz.*

1. $\begin{cases} x^2 + y^2 = z^2, \\ x^2 - y^2 = w^2. \end{cases}$ 2. $\begin{cases} x^2 + y^2 = 2z^2, \\ x^2 - y^2 = 2w^2. \end{cases}$

3. $\begin{cases} 2x^2 + y^2 = z^2, \\ 2x^2 - y^2 = w^2. \end{cases}$ 4. $\begin{cases} x^2 + 2y^2 = 2z^2, \\ x^2 - 2y^2 = 2w^2. \end{cases}$

5. $\begin{cases} x^2 + 2y^2 = z^2, \\ x^2 - 2y^2 = w^2. \end{cases}$ 6. $\begin{cases} 2x^2 + y^2 = 2z^2, \\ 2x^2 - y^2 = 2w^2. \end{cases}$

All of which are impossible forms when taken in pairs, and similar impossible forms in pairs might be deduced from like investigations; such are the following, the demonstrations of which may be made to serve for practical exercises for the student.

1. $\begin{cases} x^2 + y^2 = z^2, \\ x^2 + 2y^2 = w^2. \end{cases}$ 2. $\begin{cases} x^2 - y^2 = z^2, \\ x^2 - 2y^2 = w^2. \end{cases}$

3. $\begin{cases} x^2 + y^2 = z^2, \\ x^2 + 3y^2 = w^2. \end{cases}$ 4. $\begin{cases} x^2 - y^2 = z^2, \\ x^2 - 3y^2 = w^2. \end{cases}$

5. $\begin{cases} x^2 + 2y^2 = z^2, \\ x^2 + 3y^2 = w^2. \end{cases}$ 6. $\begin{cases} x^2 - 2y^2 = z^2, \\ x^2 - 3y^2 = w^2. \end{cases}$

7. $\begin{cases} x^2 - y^2 = z^2, \\ x^2 + 2y^2 = w^2. \end{cases}$ 8. $\begin{cases} x^2 + y^2 = z^2, \\ x^2 - 2y^2 = w^2. \end{cases}$

9. $\begin{cases} x^2 + y^2 = z^2, \\ x^2 + 4y^2 = w^2. \end{cases}$ 10. $\begin{cases} x^2 - y^2 = z^2, \\ x^2 - 4y^2 = w^2. \end{cases}$

11. $\begin{cases} x^2 + y^2 = z^2, \\ x^2 - 3y^2 = w^2. \end{cases}$ 12. $\begin{cases} x^2 - y^2 = z^2, \\ x^2 + 3y^2 = w^2, \end{cases}$

13. $\begin{cases} x^2 + 3y^2 = z^2, \\ x^2 + 4y^2 = w^2. \end{cases}$ 14. $\begin{cases} x^2 - 3y^2 = z^2, \\ x^2 - 4y^2 = w^2, \end{cases}$

And, generally, the pair of equations,

$$\begin{cases} x^2 \pm cy^2 = z^2, \\ x^2 \pm y^2 = w^2, \end{cases}$$

are impossible, if the two equations,

$$\begin{cases} m^2 \pm cn^2 = (c-1)p^2, \\ m^2 \pm n^2 = (c-1)q^2, \end{cases}$$

be impossible; and, conversely, if these last two be possible, so also are the former; the possibility or impossibility of which two last equations may be ascertained by inspection, from the table at page 104.

PROP. XIII.

57. The difference of two biquadrates cannot be equal to a square, or the equation $x^4 - y^4 = z^2$ is impossible.

For $x^4 - y^4 = (x^2 + y^2)(x^2 - y^2)$; and since we may suppose x and y to be prime to each other (art. 47), it follows, that $x^2 + y^2$ and $x^2 - y^2$ are either prime to each other, or they have only the common measure 2 (art. 8); and, therefore, since their product is a square, we must have either

$$\left.\begin{array}{l} x^2 + y^2 = r^2, \\ x^2 - y^2 = s^2, \end{array}\right\} \text{ or } \left\{\begin{array}{l} x^2 + y^2 = 2r^2, \\ x^2 - y^2 = 2s^2, \end{array}\right.$$

for otherwise their product would not be a square, or the factors would have a greater common measure than 2.

But each of these pair of forms are impossible, being the same as the forms 1 and 2 of the foregoing *scholium*; and, consequently, the equation whence they were derived is impossible also.

Q. E. D.

Cor. 1. In a similar way it may be demonstrated, that the equation $x^4+4y^4=z^2$ is impossible.

For, in this case, we must have (cor. 2, art. 54)

$$\begin{cases} x^2 = r^2 - s^2, \\ 2y^2 = 2rs, \quad \text{or } y^2 = rs. \end{cases}$$

And, since x is prime to y, r is also prime to s; and, therefore, because $rs=y^2$, r and s must be both squares; or $r=x'^2$, and $s=y'^2$, and these values, being substituted for r and s, become

$$x^2 = x'^4 - y'^4,$$

which form we have shown to be impossible in the above proposition.

Cor. 2. Hence again the equation $x^4+y^4=2z^2$ is impossible.

For $z^2=\dfrac{x^4+y^4}{2}$, or $z^4=\left(\dfrac{x^4+y^4}{2}\right)^2$; and, consequently, $z^4-x^4y^4=\left(\dfrac{x^4-y^4}{2}\right)^2$; that is, the difference of two biquadrates is equal to a square, which is impossible (art. 57).

PROP. XIV.

58. The sum of two biquadrates cannot be equal to a square, or the equation $x^4+y^4=z^2$ is impossible.

For, first, if x^4+y^4 be a square, we must have (cor. 2, art. 54)

$$\left.\begin{aligned} x^2 &= t^2 - u^2, \\ y^2 &= 2tu, \end{aligned}\right\} \text{ or } \left\{\begin{aligned} y^2 &= t^2 - u^2, \\ x^2 &= 2tu, \end{aligned}\right.$$

which are two similar expressions; and it will, therefore, be sufficient for our purpose to consider either; and as we may suppose x and y as being prime to each other (art. 47), it follows, that t and u are also prime to each other; and, consequently, since $2tu = y^2$, one of these quantities must be a square, and the other double a square (cor. 4, art. 17): let, then, $t = 2x'^2$, and $u = y'^2$, whence $t^2 - u^2 = 4x'^4 - y'^4$; that is, $x^2 = 4x'^4 - y'^4$: or, making $t = x'^2$, and $u = 2y'^2$, the equation becomes $x^2 = x'^4 - 4y'^4$; and we have, therefore, to investigate the two expressions,

$$\left\{\begin{aligned} x'^4 - 4y'^4 &= x^2, \\ 4x'^4 - y'^4 &= x^2, \end{aligned}\right.$$

one of which conditions must obtain, if the original equation be possible.

Now these are resolvible into the factors

$$\text{1st,}\quad x'^4 - 4y'^4 = (x'^2 + 2y'^2)(x'^2 - 2y'^2).$$

$$\text{2d,}\quad 4x'^4 - y'^4 = (2x'^2 + y'^2)(2x'^2 - y'^2).$$

And, since x is prime to y, and t to u, it follows, also, that x' is prime to y'; and, therefore, these factors are either prime to each other, or have only the common measure 2 (art. 8); and, consequently, since their product is a square, we must have (as in art. 57) either

$$\left.\begin{aligned} x'^2 + 2y'^2 &= r'^2, \\ x'^2 - 2y'^2 &= s'^2, \end{aligned}\right\} \text{ or } \left\{\begin{aligned} x'^2 + 2y'^2 &= 2r'^2, \\ x'^2 - 2y'^2 &= 2s'^2, \end{aligned}\right.$$

in the first case; and

$$\left.\begin{array}{l} 2x'^2+y'^2=r'^2, \\ 2x'^2-y'^2=s'^2, \end{array}\right\} \text{ or } \left\{\begin{array}{l} 2x'^2+y'^2=2r'^2, \\ 2x'^2-y'^2=2s'^2, \end{array}\right.$$

in the second.

But each of these forms, taken in pairs, has been demonstrated to be impossible (*scholium*, art. 56); and, consequently, the original equation whence they were derived is impossible also.

Cor. 1. Hence it follows, that the two equations,

$$\left\{\begin{array}{l} x^4-4y^4=z^2, \\ 4x^4-\ \ y^4=z^2, \end{array}\right.$$

are impossible, as is evident from the foregoing demonstration.

PROP. XV.

59. The area of a rational right angled triangle cannot be equal to a square.

For if it were possible, and x, y, and z, were made to represent the two sides and the hypothenuse of such a triangle, we should have

$$\left\{\begin{array}{l} x^2+y^2=z^2, \\ \ \ \frac{1}{2}xy\ =w^2. \end{array}\right.$$

Or,

$x^2+2xy+y^2=z^2+4w^2$, and $x^2-2xy+y^2=z^2-4w^2$;

that is,

$$\left\{\begin{array}{l} z^2+4w^2=(x+y)^2, \\ z^2-4w^2=(x-y)^2. \end{array}\right.$$

But these expressions cannot be both squares at the same time (art. 55); and, consequently, the area of a rational right angled triangle, cannot be equal to a square.— Q. E. D.

Cor. 1. Since, in order to have a rational right angled triangle, we must have $x^2+y^2=z^2$; it follows (from art. 54), that

$$\begin{cases} x = r^2 - s^2, \\ y = 2rs. \end{cases}$$

And, consequently, if in the fraction $\frac{r^2 - s^2}{2rs}$, or $\frac{2rs}{r^2 - s^2}$, the numerator and denominator be taken for the sides of a right angled triangle, it will be a rational one; and in these expressions we may give any values at pleasure to r and s. If, in the second fraction $\frac{2rs}{r^2 - s^2}$, we make $r = s + 1$, it becomes

$$\frac{2s^2 + 2s}{2s + 1} = s + \frac{s}{2s + 1};$$

and in this expression, by making successively

$$s = 1, \ 2, \ 3, \ 4, \ \&c.,$$

we have the following remarkable series,

$$s + \frac{s}{2s + 1} = 1\tfrac{1}{3}, \ 2\tfrac{2}{5}, \ 3\tfrac{3}{7}, \ 4\tfrac{4}{9}, \ 5\tfrac{5}{11}, \ 6\tfrac{6}{13}, \ \&c.;$$

each of which expressions, reduced to an improper fraction, gives the sides of a rational right angled triangle. And if in the fraction $\frac{r^2 - s^2}{2rs}$ we make $s = 1$, and $r = 2n + 2$, our expression becomes

$$\frac{4n^2 + 8n + 3}{4n + 4} = n + \frac{4n + 3}{4n + 4};$$

and here, making $n = 1, 2, 3, 4$, &c., we have this other series,

$$n + \frac{4n + 3}{4n + 4} = 1\tfrac{7}{8}, \ 2\tfrac{11}{12}, \ 3\tfrac{15}{16}, \ 4\tfrac{19}{20}, \ 5\tfrac{23}{24}, \ \&c.,$$

which has the same property as the former.

CHAP. V.

On the possible and impossible Forms of Cubes and Higher Powers.

PROP. I.

60. All cube numbers are of one of the forms

$$4n, \text{ or } 4n \pm 1.$$

For every number is of one of the forms

$$4n, \; 4n \pm 1, \text{ or } 4n \pm 2.$$

And the cubes of these formulæ are

$$\begin{aligned} (4n)^3 &= 64n^3 && \doteqdot 4n, \\ (4n \pm 1)^3 &= 64n^3 \pm 48n^2 + 12n \pm 1 && \doteqdot 4n \pm 1, \\ (4n \pm 2)^3 &= 64n^3 \pm 96n^2 + 48n \pm 8 && \doteqdot 4n. \end{aligned}$$

Therefore, all cubes are of one of the forms

$$4n, \text{ or } 4n \pm 1. \qquad \text{Q. E. D.}$$

Cor. 1. No number of the form $4n + 2$ is a cube.

Cor. 2. As in these forms n must be either even or odd, that is, of one of the forms $2n'$, or $2n' + 1$, the above formulæ may be again subdivided into the following:

$$\text{If } n \doteqdot 2n', \quad \begin{cases} 4n & \doteqdot 8n', \\ 4n \pm 1 & \doteqdot 8n' \pm 1. \end{cases}$$

$$\text{If } n \doteqdot 2n' + 1, \quad \begin{cases} 4n & \doteqdot 8n' + 4, \\ 4n \pm 1 & \doteqdot 8n \pm 3. \end{cases}$$

But, since $8n + 4$ is divisible by 4, and not by 8,

this form cannot contain a cube; and, therefore, all cubes to modulus 8 are of one of the forms

$$8n, \ 8n \pm 1, \text{ or } 8n \pm 3.$$

Cor. 3. No numbers of the form $8n+2$, $8n+4$, or $8n+6$, are cubes.

PROP. II.

61. All cube numbers are of one of the forms

$$7n, \text{ or } 7n \pm 1.$$

For every number is of one of the forms

$$7n, \ 7n \pm 1, \ 7n \pm 2, \ 7n \pm 3.$$

And the cubes of these formulæ take the following forms; *viz.*

$$\begin{aligned}
&(7n)^3 \text{ - - - - - - - - - - - - - - } \doteqdot 7n,\\
&(7n \pm 1)^3 = 7^3n^3 \pm 3 \,.\, 7^2n^2 + 3 \,.\, 7n \pm 1 \doteqdot 7n \pm 1,\\
&(7n \pm 2)^3 = 7^3n^3 \pm 3 \,.\, 2 \,.\, 7^2n^2 + 3 \,.\, 2^2 \, 7n \pm 8 \doteqdot 7n \pm 1,\\
&(7n \pm 3)^3 = 7^3n^3 \pm 3 \,.\, 3 \,.\, 7^2n^2 + 3 \,.\, 3^2 \,.\, 7n \pm 27 \doteqdot 7n \pm 1.
\end{aligned}$$

Therefore, all cube numbers are of the forms

$$7n, \text{ or } 7n \pm 1. \qquad \text{Q. E. D.}$$

Cor. 1. No numbers of the forms $7n+2$, $7n+3$, $7n+4$, $7n+5$, can be cubes.

Cor. 2. If a cube number be divisible by 7, it is also divisible by 7^3. And, conversely, if a number be divisible by 7, and not also divisible by 7^3, that number is not a cube.

Cor. 3. As n, in the above forms, must be either even or odd, we may subdivide these into the following:

$$n \doteqdot 2n', \qquad \begin{cases} 7n \doteqdot 14n', \\ 7n \pm 1 \doteqdot 14n' \pm 1. \end{cases}$$

$$n \doteqdot 2n'+1, \begin{cases} 7n \quad\;\; \doteqdot 14n' \pm 7, \\ 7n \pm 1 \doteqdot 14n' \pm 6. \end{cases}$$

Therefore, all cubes to modulus 14 are of one of the forms, $14n$, $14n \pm 1$, $14n \pm 7$, $14n \pm 6$. And, conversely, no numbers of the form $14n+2$, $14+3$, $14n+4$, $14n+5$, $14n+9$, $14n+10$, $14n+11$, $14n+12$, can be cube numbers.

PROP. III.

62. All cube numbers are of one of the forms

$$9n, \text{ or } 9n \pm 1.$$

For all numbers to modulus 9 must fall under one or other of the following forms, *viz.* $9n$, $9n \pm 1$, $9n \pm 2$, $9n \pm 3$, $9n \pm 4$; the cubes of which give

$$(9n \quad)^3 \text{ - - - - - - - - - - } \doteqdot 9n,$$
$$(9n \pm 1)^3 = 9^3n^3 \pm 3 \,.\; 9^2n^2 + 3 \,.\; 9n \pm 1 \doteqdot 9n \pm 1,$$
$$(9n \pm 2)^3 = 9^3n^3 \pm 3 \,.\, 2 \,.\, 9^2n^2 + 3 \,.\, 2^2 \,.\, 9n \pm 8 \doteqdot 9n \pm 1,$$
$$(9n \pm 3)^3 = 9^3n^3 \pm 3 \,.\, 3 \,.\, 9^2n^2 + 3 \,.\, 3^2 \,.\, 9n \pm 27 \doteqdot 9n,$$
$$(9n \pm 4)^3 = 9^3n^3 \pm 3 \,.\, 4 \,.\, 9^2n^2 + 3 \,.\, 4^2 \,.\, 9n \pm 64 \doteqdot 9n \pm 1.$$

Therefore, all cubes are of one of the forms

$9n$, or $9n \pm 1$. Q. E. D.

Cor. 1. No numbers of the form $9n+2$, $9n+3$, $9n+4$, $9n+5$, $9n+6$, $9n+7$ can be cubes.

Cor. 2. By applying here the same reasoning as in the corollary above, we shall find, that all cube numbers to modulus 18 are of one of the forms $18n$, $18n \pm 1$, $18n \pm 8$, $18n \pm 9$; and, therefore, conversely, no number in any of the forms $18n+2$, $18n+3$, $18n+4$, $18n+5$, $18n+6$, $18n+7$,

$18n+11$, $18n+12$, $18n+13$, $18n+14$, $18n+15$, $18n+16$, can be a cube.

PROP. IV.

63. All cube numbers are of the same form to any modulus a, as the cubes

$$0^3, 1^3, 2^3, 3^3, \&c., (a-1)^3.$$

For every number N may be represented by the formula $an+r$, in which $r < a$ (art. 11). But

$$(an+r)^3 = a^3n^3 + 3a^2n^2r + 3anr^2 + r^3 =$$
$$a(a^2n^3 + 3an^2r + 3nr^2) + r^3,$$

and is, therefore, of the same, form when compared by modulus a, as the cube r^3; because all the other part of the formula is divisible by a; but since $r < a$, it must be one of the terms in the series

$$1, 2, 3, 4, \&c., (a-1);$$

and, consequently, all cubes are of the same form to any particular modulus a, as the cubes

$$0^3, 1^3, 2^3, 3^3, \&c., (a-1)^3. \qquad \text{Q. E. D.}$$

Cor. 1. Hence, in order to ascertain the forms of cube numbers to any given modulus a, we need only find those of all the cubes less than a; that is, of the series

$$0^3, 1^3, 2^3, 3^3, \&c., (a-1)^3:$$

and hence a table of those forms might be readily constructed; but as, in many cases, the number of forms would be equal to the number expressing the modulus, no advantage could be derived from the classification, because no numbers are in these cases excluded; thus, to modulus 10 we should have the ten forms $10n$, $10n+1$, $10n+2$, $10n+3$,

$10n+4$, $10n+5$, $10n+6$, $10n+7$, $10n+8$, $10n+9$; so that no number is excluded with this modulus; and hence it appears, that cube numbers may terminate with any of the digits, whereas in squares we have seen (cor. 5, art. 43), that they always terminate in 0, 1, 4, 5, 6, or 9.

PROP. V.

64. All cube numbers, with regard to modulus 6, are of the same forms as their roots.

For all numbers are of one of the forms $6n$, $6n+1$, $6n+2$, $6n+3$, $6n+4$, $6n+5$; and the cubes of these formulæ will evidently take the following forms:

$$\left.\begin{array}{l}(6n+0)^3,\\(6n+1)^3,\\(6n+2)^3,\\(6n+3)^3,\\(6n+4)^3,\\(6n+5)^3,\end{array}\right\}\text{ the same form as }\left\{\begin{array}{l}0^3 \pm 6n+0;\\1^3 \pm 6n+1;\\2^3 \pm 6n+2;\\3^3 \pm 6n+3;\\4^3 \pm 6n+4;\\5^3 \pm 6n+5:\end{array}\right.$$

which are manifestly the same forms as the cubes that they represent.

Cor. Hence the difference between any integral cube and its root, is always divisible by 6.

PROP. VI.

65. The equation $(4p+2)t^3 \pm 4qu^3 = w^3$ is always impossible in integers, while q is prime to 4.

For (cor. art. 47) the three cubes t^3, u^3, and w^3, may be considered as prime to each other. Also all cubes are of one of the forms $4n$, or $4n \pm 1$ (art. 60); and, since $4qu^3$ is always of the form $4n$,

whatever may be the form of u^3, we shall have, in the first place, by making $t^3 \doteq 4n$,

$$(4p+2)4n \pm 4qu^3 = w^3 \doteq 4n';$$

that is, t^3 and w^3 both of the form $4n$, which is absurd, because they are prime to each other by hypothesis.

Again, if $t^3 \doteq 4n \pm 1$, we have

$$(4p+2)(4n \pm 1) \pm 4qu^3 = w^3, \text{ or}$$
$$16p + 8n \pm 4p \pm 2 \pm 4qu^3 = w^3, \text{ or}$$
$$4(4p + 2n \pm p \pm qu^3) \pm 2 = w^3; \text{ that is,}$$
$$w^3 \doteq 4n + 2,$$

which is an impossible form for cubes (cor. 1, art. 60); and, consequently, the equation

$$(4p+2)t^3 \pm 4qu^3 = w^3,$$

is impossible, while q is prime to 4. — Q. E. D.

The condition of q being prime to 4 is evidently necessary; for if q had the form $2q'$, then the equation would become $(4p+2)t^3 \pm q' \cdot (2u)^3 = w^3$, and the possibility or impossibility would depend upon the form of q', and would, therefore, require a different mode of demonstration; hence, in this, and also in the following propositions, q must always be taken prime to the respective modulus with which it enters.

Cor. 1. By means of the general formula above given, we derive the following particular cases, which are all impossible in integers, q being taken prime to 4.

$2t^3 \pm 4u^3 = w^3$,	$2t^3 \pm 12u^3 = w^3$,
$6t^3 \pm 4u^3 = w^3$,	$6t^3 \pm 12u^3 = w^3$,
$10t^3 \pm 4u^3 = w^3$,	$10t^3 \pm 12u^3 = w^3$,
&c. &c. &c.	&c. &c. &c.

And it is obvious how these may be extended to any length at pleasure; and others may be found by taking $q=5, 7, 9$, &c.

PROP. VII.

66. The two general equations,

$$\begin{cases} (7p \pm 2)t^3 \pm 7qu^3 = w^3, \\ (7p \pm 3)t^3 \pm 7qu^3 = w^3, \end{cases}$$

are impossible in integers, while q is prime to 7.

For we may, as before, consider t^3, u^3, and w^3, as prime to each other. And since it has been shown (art. 61), that all cube numbers are of one of the forms $7n$, or $7n \pm 1$; and, because $7qu^3$ is always of the form $7n$, we need only give to t^3 the two forms $7n$, or $7n \pm 1$, to ascertain the possibility or impossibility of the above equations. But in the case of $t^3 \doteq 7n$, it is evident, that w^3 would then have the same form $7n$; so that t^3 and w^3, being both of the form $7n$, would not be prime to each other, which is contrary to the hypothesis; and, therefore, if the equations be possible, it must be when $t^3 \doteq 7n \pm 1$: let us, therefore, investigate the equations upon this supposition.

Suppose, then, $t^3 \doteq 7n \pm 1$; whence the first equation becomes

$$\begin{aligned} (7p \pm 2)(7n \pm 1) \pm 7qu^3 &= w^3, \text{ or} \\ 49pn \pm 14n \pm 7p \pm 2 \pm 7qu^3 &= w^3, \text{ or} \\ 7(7pn \pm 2n \pm p \pm qu^3) \pm 2 &= w^3, \text{ or} \\ w^3 &\doteq 7n \pm 2; \end{aligned}$$

which we have seen (cor. 1, art. 61) is an impossible form for cubes; and, consequently, the first equation is impossible.

In the second equation, by giving t^3 the same form, we have

$$\begin{aligned}
(7p \pm 3)t^3 \pm 7qu^3 &= w^3, \text{ or} \\
(7p \pm 3)(7n \pm 1) \pm 7qu^3 &= w^3, \text{ or} \\
49pn \pm 21n \pm 7p \pm 3 \pm 7qu^3 &= w^3, \text{ or} \\
7(7pn \pm 3n \pm p \pm qu^3) \pm 3 &= w^3, \text{ or} \\
w^3 &= 7n \pm 3,
\end{aligned}$$

which is an impossible form (cor. 1, art. 61); and, therefore, both the original equations are impossible. — Q. E. D.

Cor. 1. By means of these general formulæ are readily deduced the following particular cases:

$2t^3 \pm 7u^3 = w^3,$	$2t^3 \pm 14u^3 = w^3,$
$3t^3 \pm 7u^3 = w^3,$	$3t^3 \pm 14u^3 = w^3,$
$4t^3 \pm 7u^3 = w^3,$	$4t^3 \pm 14u^3 = w^3,$
$5t^3 \pm 7u^3 = w^3,$	$5t^3 \pm 14u^3 = w^3,$
$9t^3 \pm 7u^3 = w^3,$	$9t^3 \pm 14u^3 = w^3,$
$10t^3 \pm 7u^3 = w^3,$	$10t^3 \pm 14u^3 = w^3,$
&c. &c. &c.	&c. &c. &c.

Which are impossible forms for cubes, and they may be farther extended by giving other values to p and q, observing to take q prime to 7.

PROP. VIII.

67. The three general equations,

$$\begin{cases} (9p \pm 2)t^3 \pm 9qu^3 = w^3, \\ (9p \pm 3)t^3 \pm 9qu^3 = w^3, \\ (9p \pm 4)t^3 \pm 9qu^3 = w^3, \end{cases}$$

are all impossible in integers, q being taken prime to the modulus 9.

For here again we may suppose t^3, u^3, and w^3, as being prime to each other; also, $9qu^3$ is always of the form $9n$, whatever be the form of u^3: it is, there-

fore, only necessary to investigate the possibility or impossibility of the three given equations, under the different forms of t^3; *viz.* when $t^3 \doteq 9n$, and $t^3 \doteq 9n \pm 1$.

Now, with regard to the first, *viz.* $t^3 \doteq 9n$, we see immediately, that in all the equations, w^3 would have the same form $9n$; and, therefore, t^3 and w^3 would thus have a common divisor, which is contrary to the hypothesis, as all the three cubes are prime to each other; and, consequently, if the equations be possible, it must be when $t^3 \doteq 9n \pm 1$.

Now, this form being substituted for t^3, we have,

First equation,

$$\begin{aligned}
(9p \pm 2)t^3 \pm 9qu^3 &= w^3, \text{ or} \\
(9p \pm 2)(9n \pm 1) \pm 9qu^3 &= w^3, \text{ or} \\
81pn \pm 18n \pm 9p \pm 2 \pm 9qu^3 &= w^3, \text{ or} \\
9(9pn \pm 2n \pm p \pm qu^2) \pm 2 &= w^2, \text{ or} \\
w^3 \doteq 9n \pm 2,&
\end{aligned}$$

which is an impossible form for cubes (cor. 1, art. 62); and, therefore, the first equation is impossible.

The second equation gives

$$\begin{aligned}
(9p \pm 3)t^3 \pm 9qu^3 &= w^3, \text{ or} \\
(9p \pm 3)(9n \pm 1) \pm 9qu^3 &= w^3, \text{ or} \\
81pn \pm 27n \pm 9p \pm 3 \pm 9qu^3 &= w^3, \text{ or} \\
9(9pn \pm 3n \pm p \pm qu^3) \pm 3 &= w^3, \text{ or} \\
w^3 \doteq 9n \pm 3,&
\end{aligned}$$

which is likewise an impossible form for cubes (cor. 1, art. 62); and, therefore, the second equation is impossible.

In the third equation, we have,

$$(9p \pm 4)t^3 \pm 9qu^3 = w^3, \text{ or}$$
$$(9p \pm 4)(9n \pm 1) \pm 9qu^3 = w^3, \text{ or}$$
$$81pn \pm 36n \pm 9p \pm 4 \pm 9qu^3 = w^3, \text{ or}$$
$$9(9pn \pm 4n \pm p \pm qu^3) \pm 4 = w^3, \text{ or}$$
$$w^3 \doteq 9n \pm 4,$$

which is also an impossible form for cubes (cor. 1, art. 62); and, consequently, the third equation, as well as the first and second, is impossible.—Q. E. D.

Cor. The above three general equations furnish the following particular cases of impossible forms of cubes:

$2t^3 \pm 9u^3 = w^3$,	$2t^3 \pm 18u^3 = w^3$,
$3t^3 \pm 9u^3 = w^3$,	$3t^3 \pm 18u^3 = w^3$,
$4t^3 \pm 9u^3 = w^3$,	$4t^3 \pm 18u^3 = w^3$,
$5t^3 \pm 9u^3 = w^3$,	$5t^3 \pm 18u^3 = w^3$,
$6t^3 \pm 9u^3 = w^3$,	$6t^3 \pm 18u^3 = w^3$,
$7t^3 \pm 9u^3 = w^3$,	$7t^3 \pm 18u^3 = w^3$,
$11t^3 \pm 9u^3 = w^3$,	$11t^3 \pm 18u^3 = w^3$,
&c. &c. &c.	&c. &c. &c.

Which, like the other tables of impossible forms, may be carried to any length at pleasure, by giving different values to p and q; observing always, that q is prime to modulus 9.

PROP. IX.

68. If there be any case in which the equation $x^3 - y^3 = z^3$ be possible, the following conditions must obtain; *viz.*

$$\begin{cases} x - y \doteq r^3, \\ x - z \doteq s^3, \\ y + z \doteq t^3; \end{cases}$$

or two of these quantities will be of the form here

given, and the other of the form $9\phi^3$, which resolve into the four following cases; *viz.*

$$1\text{st}, \begin{cases} x-y \mp r^3, \\ x-z \mp s^3, \\ y+z \mp t^3. \end{cases} \qquad 2\text{d}, \begin{cases} x-y \mp 9r^3, \\ x-z \mp s^3, \\ y+z \mp t^3, \end{cases}$$

$$3\text{d}, \begin{cases} x-y \mp r^3, \\ x-z \mp 9s^3, \\ y+z \mp t^3. \end{cases} \qquad 4\text{th}, \begin{cases} x-y \mp r^3, \\ x-z \mp s^3, \\ y+z \mp 9t^3. \end{cases}$$

And it is to be demonstrated, that one of these four conditions must obtain, if the equation $x^3-y^3=z^3$ be possible; where r^3, s^3, and t^3, may be any numbers whatever, indicating only that $x-y$, $x-z$, $y+z$, are complete cubes, or that they are of the forms there given.

In the first place, we may consider x, y, and z, as being prime to each other (cor. art. 47); and since $x>y$, put $x=y+d$; then, because x is prime to y, d is prime both to x and y, for if y and d had a common measure, x would have the same, because $x=y+d$; and if x and d had a common measure, y would have the same, because $y=x-d$; and, therefore, since x and y have no common measure, d is prime both to x and y.

Now, substituting $y+d$ instead of x, in the given equation, it becomes

$$(y+d)^3-y^3 = z^3, \text{ or}$$
$$3y^2d+3yd^2+d^3=z^3, \text{ or}$$
$$d(3y^2+3yd+d^2)=z^3.$$

And here, since d is prime to y, it follows, that the first side of this equation is divisible by d *once*, and after that, neither by d nor by any factor of d, unless 3 be one of its factors, in which case it is divisible by $3d$ *once*, and after that, neither by d

nor by any factor of d. For of the three terms $(3y^2+3yd+d^2)$, which form the quotient, two of them have d enter into their composition, and are therefore divisible by d; but in the other term, y^2 is prime to d, and, consequently, the whole quantity taken collectively is also prime to d, unless 3 be one of the factors of d, in which case, as we have said above, the first side will have $3d$ for a divisor, but after that, the quotient will be prime to d; and whatever is true of the first side of the equation is evidently so of the other side z^3, because they are equal quantities; and, consequently, z^3 is divisible by d *once*, and after that neither by d nor by any factor of d, unless 3 be one of its factors; in which case, it is divisible by $3d$ *once*, and after that neither by d nor by any factor of d: and, therefore, d in the first case, and $3d$ in the second, must be complete cubes (cor. 1, art. 16); that is, we must have either $d = r^3$, or $d = 9r^3$, in order that $3d = 3^3r^3$: or, since $d = x - y$, it follows that $x - y = r^3$, or $9r^3$.

Now if the equation $x^3 - y^3 = z^3$ be possible, so likewise is $x^3 - z^3 = y^3$, and it is evident, that, were we to consider the equation under this form, the result would be exactly similar to that obtained above; *viz.* $x - z$ must be of one of the forms s^3, or $9s^3$.

Again, the same equation, by transposition, becomes

$$y^3 + z^3 = x^3.$$

And making $y + z = m$, or $y = m - z$, we have

$$(m - z)^3 + z^3 = x^3,$$

where m is prime both to z and y; for, if m and z had a common measure, y would have the same, because

$m-z=y$; and, if m and y had a common measure, z must have the same, because $m-y=z$; and, consequently, since y and z are prime to each other, it follows, that m is prime both to y and z. Now, by cubing $(m-z)$ in the above equation, it becomes

$$m^3-3m^2z+3mz^2 = x^3, \text{ or}$$
$$m(m^2-3mz+3z^2)=x^3.$$

And hence, by exactly the same chain of reasoning as that employed in the foregoing part of the proposition, it follows, that m is of one of the forms t^3, or $9t^3$; or, since $m=y+z$, we have $y+z \doteq t^3$, or $9t^3$. And hence it follows, that, if there be any case in which the equation

$$x^3-y^3=z^3$$

be possible, the following conditions must obtain; *viz.*

$$x-y \doteq r^3, \text{ or } 9r^3;$$
$$x-z \doteq s^3, \text{ or } 9s^3;$$
$$y+z \doteq t^3, \text{ or } 9t^3.$$

But since $x-y$, $x-z$, and $y+z$, are respectively the divisors of the three cubes z^3, y^3, and x^3, and these quantities being prime to each other, their divisors are also necessarily prime to each other; and, therefore, only one of these quantities can be of the latter forms above given, for if two of them were of the second forms, they would have a common measure 3, which is impossible, since they are prime to each other. Consequently, if the equation

$$x^3-y^3=z^3$$

be possible, we must have,

$$x-y \mp r^3,$$
$$x-z \mp s^3,$$
$$y+z \mp t^3.$$

Or two of these quantities must have this form, and the third the form $9\phi^3$, which evidently resolves into the four following cases, one of which conditions must necessarily obtain, if the equation

$$x^3 - y^3 = z^3$$

be possible; *viz.*

$$\text{1st, } \begin{cases} x-y \mp r^3, \\ x-z \mp s^3, \\ y+z \mp t^3. \end{cases} \qquad \text{2d, } \begin{cases} x-y \mp 9r^3, \\ x-z \mp s^3, \\ y+z \mp t^3. \end{cases}$$

$$\text{3d, } \begin{cases} x-y \mp r^3, \\ x-z \mp 9s^3, \\ y+z \mp t^3. \end{cases} \qquad \text{4th, } \begin{cases} x-y \mp r^3, \\ x-z \mp s^3, \\ y+z \mp 9t^3. \end{cases}$$

Q. E. D.

We have only considered the equation $x^3 - y^3 = z^3$, but this evidently includes the more general form $x^3 \pm y^3 = z^3$; for if the ambiguous sign be taken $+$, it becomes $x^3 + y^3 = z^3$, or $z^3 - y^3 = x^3$, which is the form that has been investigated, the only difference being the change of the letter z for x.

PROP. X.

69. The sum or difference of two cubes cannot be equal to a cube, or the equation

$$x^3 \pm y^3 = z^3$$

is always impossible, either in integers or fractions.

First, from what has been observed above, it will be sufficient to consider the equation under the form $x^3 - y^3 = z^3$, which involves the two forms

$$x^3 \pm y^3 = z^3;$$

except in the change of one letter for another; we shall, therefore, only investigate the equation under the limited form $x^3-y^3=z^3$, which, being proved impossible, will necessarily involve the impossibility of the general equation $x^3 \pm y^3 = z^3$. Now by the foregoing proposition, if the equation be possible, one of the four following conditions must obtain*; *viz.*

$$1\text{st}, \begin{cases} x-y= r^3, \\ x-z= s^3, \\ y+z= t^3. \end{cases} \qquad 2\text{d}, \begin{cases} x-y=9r^3, \\ x-z= s^3, \\ y+z= t^3. \end{cases}$$

$$3\text{d}, \begin{cases} x-y= r^3, \\ x-z=9s^3, \\ y+z= t^3. \end{cases} \qquad 4\text{th}, \begin{cases} x-y= r^3, \\ x-z= s^3, \\ y+z=9t^3. \end{cases}$$

But at present it will be sufficient to consider one of those cases; for example, the first; and in our result, by substituting $9r^3$ for r^3, $9s^3$ for s^3, or $9t^3$ for t^3; we shall evidently have the results in each of the four cases.

First, then, let us endeavour to ascertain, whether the equation be possible, upon the supposition that

$$\begin{cases} x-y=r^3, \\ x-z=s^3, \\ y+z=t^3. \end{cases}$$

Now from these three equations we obtain the three following ones; *viz.*

$$x=\tfrac{1}{2}\{t^3+(s^3+r^3)\},$$
$$y=\tfrac{1}{2}\{t^3+(s^3-r^3)\},$$
$$z=\tfrac{1}{2}\{t^3-(s^3-r^3)\}.$$

And, consequently, since

$x^3-y^3=z^3$, or $x^3=y^3+z^3$, we have

* Since the above quantities are of these forms they may be made $=r^3, s^3,$ &c.

$$\left(\frac{t^3+(s^3+r^3)}{2}\right)^3=\left(\frac{t^3+(s^3-r^3)}{2}\right)^3+\left(\frac{t^3-(s^3-r^3)}{2}\right)^3.$$

Or,

$$\{t^3+(s^3+r^3)\}^3=\{t^3+(s^3-r^3)\}^3+\{t^3-(s^3-r^3)\}^3.$$

Again,

$$\{t^3+(s^3+r^3)\}^3=\left\{\begin{array}{l} t^9+3t^6(s^3+r^3)+3t^3(s^3+r^3)^2+ \\ \quad (s^3+r^3)^3. \end{array}\right.$$

$$\{t^3+(s^3-r^3)\}^3=\left\{\begin{array}{l} t^9+3t^6(s^3-r^3)+3t^3(s^3-r^3)^2+ \\ \quad (s^3-r^3)^3. \end{array}\right.$$

$$\{t^3-(s^3-r^3)\}^3=\left\{\begin{array}{l} t^9-3t^6(s^3-r^3)+3t^3(s^3-r^2)^2- \\ \quad (s^3-r^3)^3. \end{array}\right.$$

And subtracting the first equation from the sum of the two latter, to which it is equal, we have

$$\left\{\begin{array}{l} t^9-3t^6(s^3+r^3)+3t^3\{2(s^3-r^3)^2-(s^3+r^3)^2\}- \\ \quad (s^3+r^3)^3=0;\ \text{or} \end{array}\right.$$

$$\left\{\begin{array}{l} t^9-3t^6(s^3+r^3)+3t^3(s^3+r^3)^2-(s^3+r^3)^3= \\ \quad 24t^3s^3r^3,\ \text{because} \end{array}\right.$$

$$2(s^3-r^3)^2+8s^3r^3=2(s^3+r^3)^2,\ \text{whence}$$

$$\{t^3-(s^3+r^3)\}^3=24t^3s^3r^3.$$

And here the impossibility of the equation is manifest, under the present supposition; because we have got an integral cube, equal to three times another integral cube, which is absurd. But by substituting $9r^3$ for r^3, $9s^3$ for s^3, and $9t^3$ for t^3, the impossibility is not so immediately obvious; for, in these cases, by putting $9r^3$ for r^3, we have

$$\{t^3-(s^3+9r^3)\}^3=216t^3s^3r^3=(6tsr)^3.$$

Again, writing $9s^3$ for s^3, we obtain

$$\{t^3-(9s^3+r^3)\}^3=216t^3s^3r^3=(6tsr)^3.$$

And $9t^3$ for t^3 gives

$$\{9t^3-(s^3+r^3)\}^3=216t^3s^3r^3=(6tsr)^3.$$

And it here remains to be shown, that these equalities cannot subsist.

Now these equations, by extraction, become,

$$1\text{st},\quad t^3 - s^3 - 9r^3 = 6tsr.$$
$$2\text{d},\quad t^3 - 9s^3 - r^3 = 6tsr.$$
$$3\text{d},\quad 9t^3 - s^3 - r^3 = 6tsr.$$

Whence, again, by division, we have

$$1\text{st},\quad \frac{t^2}{sr} - \frac{s^2}{tr} - \frac{9r^2}{st} = 6.$$
$$2\text{d},\quad \frac{t^2}{sr} - \frac{9s^2}{tr} - \frac{r^2}{st} = 6.$$
$$3\text{d},\quad \frac{9t^2}{sr} - \frac{s^2}{tr} - \frac{r^2}{st} = 6.$$

And one of these equations must be possible, if the equation whence they were derived be so.

But, since r, s, and t, are prime to each other, each of the above fractions is in its simplest form; and they each contain a factor in their denominator, that is not common with the other denominators; and, therefore, these fractions cannot any how combined be equal to an integer (cor. 2, art. 13).

Having therefore shown, that if the equation $x^3 - y^3 = z^3$ were possible, one of the above expressions must be equal to the integer 6; and having also demonstrated, that these fractions cannot be equal to any integer whatever, or that the above equalities are impossible; it therefore necessarily follows, that the equation whence they were derived is so likewise; that is, the equation $x^3 - y^3 = z^3$ is impossible: but the impossibility of the equation $x^3 - y^3 = z^3$ involves in it the impos-

sibility of the general equation $x^3 \pm y^3 = z^3$; and, consequently, the equation

$$x^3 \pm y^3 = z^3$$

is impossible in integral numbers. — Q. E. D.

Cor. Since $x^3 \pm y^3 = z^3$ is impossible, so likewise is $\frac{x^3}{p^3} \pm \frac{y^3}{q^3} = \frac{z^3}{r^3}$, for this may be reduced to

$$q^3x^3 \pm p^3y^3 = \frac{z^3p^3q^3}{r^3},$$

where the latter cube must be an integer, which we have seen is impossible; therefore, the equation cannot obtain, either in integers or fractions.

PROP. XI.

70. The third differences of consecutive cube numbers are constant, and equal to $1 \cdot 2 \cdot 3 = 6$.

For let $(x-1)^3$, x^3, $(x+1)^3$, $(x+2)^3$, represent any four consecutive cubes, then

$$\begin{aligned} (x-1)^3 &= x^3 - 3x^2 + \ \ 3x - 1, \\ x^3 &= x^3, \\ (x+1)^3 &= x^3 + 3x^2 + \ \ 3x + 1, \\ (x+2)^3 &= x^3 + 6x^2 + 12x + 8. \end{aligned}$$

$$\text{1st differences, } \begin{cases} 3x^2 - 3x + 1, \\ 3x^2 + 3x + 1, \\ 3x^2 + 9x + 7. \end{cases}$$

$$\text{2d differences, } \begin{cases} 6x, \\ 6x + 6. \end{cases}$$

$$\text{3d difference, } = 6 = 1 \cdot 2 \cdot 3. \qquad \text{Q. E. D.}$$

Cor. 1. In the same manner it may be shown, that the third differences of cubes, the roots of which are in arithmetical progression, are equal to

$1 \,.\, 2 \,.\, 3 \,.\, d^3$, where d is the common difference of the roots.

Cor. 2. The second differences of consecutive squares are equal to 2; or to $2d^2$, if their roots form an arithmetical series, whose common difference is d; which is readily demonstrated on the same principles as those employed above.

PROP. XII.

71. Every complete biquadrate, or 4th power, is of one of the forms $5n$, or $5n+1$.

This is evident, for every square number is of one of the forms $5n$, or $5n \pm 1$; and a 4th power being the square of a square, we have

$$(5n\quad)^2 = 5^2n^2 \qquad\qquad \doteqdot 5n,$$
$$(5n \pm 1)^2 = 5^2n^2 \pm 10n + 1 \doteqdot 5n + 1;$$

therefore, every 4th power is of one of the forms $5n$, or $5n+1$.— Q. E. D.

Cor. 1. If a 4th power be divisible by 5, it is also divisible by 5^4. And, conversely, if a number be divisible by 5, and not by 5^4, that number is not a 4th power.

Cor. 2. No number of the form $5n+2$, or $5n+3$, or $5n+4$, is a biquadrate.

Cor. 3. Every 4th power being of one of the forms $5n$, or $5n+1$, we have, by supposing n even and odd, the four following forms to modulus 10; *viz.*

$$n \doteqdot 2n' \quad \begin{cases} 5n \doteqdot 10n', \\ 5n+1 \doteqdot 10n'+1; \end{cases}$$
$$n \doteqdot 2n'+1 \begin{cases} 5n \doteqdot 10n'+5, \\ 5n+1 \doteqdot 10n'+6; \end{cases}$$

and hence every 4th power terminates with one of

the digits, 0, 1, 5, or 6. And, conversely, no number terminating in 2, 3, 4, 7, 8, or 9, is a biquadrate.

Cor. 4. Since it is demonstrated (cor. 2, art. 42), that all even squares are of the form $4n$, and all odd squares of the form $8n+1$, we have for the squares of these

$$(4n\quad)^2 = 16n^2 \qquad\qquad = 16n',$$
$$(8n+1)^2 = 64n^2 + 16n + 1 = 16n' + 1.$$

And, consequently, every complete 4th power is of one of the forms $16n$, or $16n+1$; that is, every even 4th power is of the form $16n$, and every odd 4th power of the form $16n+1$.

PROP. XIII.

72. All 4th powers are of the same form with regard to any number a as a modulus, as the 4th powers

$$0^4,\ 1^4,\ 2^4,\ 3^4,\ \&c.,\ (\tfrac{1}{2}a)^4,$$

when a is even; and as

$$0^4,\ 1^4,\ 2^4,\ 3^4,\ \&c.,\ \left(\frac{a-1}{2}\right)^4,$$

when a is odd.

For every number whatever may be represented by the formula $an \pm r$, where r never exceeds $\frac{1}{2}a$ (art. 10). But

$$(an \pm r)^4 = a^4n^4 \pm 4a^3n^3r + 6a^2n^2r^2 \pm 4anr^3 + r^4,$$

and all the terms, but the last, of this expression, being divisible by a, the whole quantity is evidently of the same form, with regard to a as a modulus, as the last term r^4; but r never exceeds $\frac{1}{2}a$, therefore,

every 4th power to modulus a is of the same form as the 4th powers

0^4, 1^4, 2^4, 3^4, &c., $(\frac{1}{2}a)^4$, when a is even; and as

$$0^4,\ 1^4,\ 2^4,\ 3^4,\ \&c.,\ \left(\frac{a-1}{2}\right)^4, \text{ when } a \text{ is odd.}$$

Q. E. D.

Scholium. By means of this proposition, we readily compute the following table for 4th powers, which exhibits all the possible forms to every modulus, from 2 to 12.

Table of the Forms under which all 4th Powers are contained, to every Modulus, from 2 *to* 12.

Moduli.	*Forms.*					
2	$2n$	$2n+1$				
3	$3n$	$3n+1$				
4	$4n$	$4n+1$				
5	$5n$	$5n+1$				
6	$6n$	$6n+1$	$6n+3$	$6n+4$		
7	$7n$	$7n+1$	$7n+2$	$7n+4$		
8	$8n$	$8n+1$				
9	$9n$	$9n+1$	$9n+4$	$9n+7$		
10	$10n$	$10n+1$	$10n+5$	$10n+6$		
11	$11n$	$11n+1$	$11n+3$	$11n+4$	$11n+5$	$11n+9$
12	$12n$	$12n+1$	$12n+4$	$12n+9$		

And hence, by way of exclusion, arises the following

Table of impossible Forms for Biquadrates, or 4th Powers.

Moduli.	Impossible Forms.					
3	$3n+2$					
4	$4n+2$	$4n+3$				
5	$5n+2$	$5n+3$	$5n+4$			
6	$6n+2$	$6n+5$				
7	$7n+3$	$7n+5$	$7n+6$			
8	$8n+2$	$8n+3$	$8n+4$	$8n+5$	$8n+6$	$8n+7$
9	$9n+2$	$9n+3$	$9n+5$	$9n+6$	$9n+8$	
10	$10n+2$	$10n+3$	$10n+4$	$10n+7$	$10n+8$	$10n+9$
11	$11n+2$	$11n+4$	$11n+6$	$11n+7$	$11n+8$	$11n+10$
12	$12n+2$	$12n+3$	$12n+5$	$12n+6$	$12n+7$	$12n+8$
		$12n+10$	$12n+11$			

These tables are sometimes useful in ascertaining the possibility of equations of the form $x^4 \pm ay^4 = z^4$.

PROP. XIV.

73. The two indeterminate equations

$$\begin{cases} x^4 \pm \quad y^4 = z^4, \\ x^4 \pm a^2y^4 = z^4, \end{cases}$$

are both impossible.

For we have seen (arts. 57 and 58), that the equation $x^4 \pm y^4 = z^2$ is impossible in integers; and, therefore, *a fortiori*, the equation $x^4 \pm y^4 = z^4$ is also impossible.

Again, we have, by transposition, in the second equation,

$$x^4 - z^4 = (ay^2)^2,$$

which is also impossible (art. 57); and, consequently, the two given equations are impossible in integers.— Q. E. D.

Cor. Hence it follows, that the equation

$$x^4 \pm 4y^4 = z^4$$

is impossible, because we have demonstrated (cor. 1, arts. 57 and 58), that $x^4 \pm 4y^4 = z^2$ is impossible. Also the equation $x^4 + y^4 = 2z^4$ is impossible (cor. 2, art. 57).

On similar principles it is evident, that both the equations

$$\begin{cases} 2x^4 - y^4 = z^4, \\ 4x^4 - y^4 = z^4, \end{cases}$$

are impossible; by the same arts. and cors.

PROP. XV.

74. The three general equations

$$\begin{cases} (5p+2)t^4 \mp 5qu^4 = w^4, \\ (5p+3)t^4 \mp 5qu^4 = w^4, \\ (5p+4)t^4 + 5qu^4 = w^4, \end{cases}$$

are impossible, q being taken prime to 5.

For, in the first place, we may always consider t^4, u^4, and w^4, as prime to each other (cor., art. 47).

And since all 4th powers are of one of the forms $5n$, or $5n+1$, we shall have, by giving to t^4 these forms, the following equations:

If $t^4 \doteq 5n$,

$$1. \begin{cases} (5p+2) \times 5n \mp 5qu^4 = w^4 \doteq 5n', \\ (5p+3) \times 5n \mp 5qu^4 = w^4 \doteq 5n', \\ (5p+4) \times 5n + 5qu^4 = w^4 \doteq 5n'. \end{cases}$$

And if $t^4 \doteq 5n+1$,

$$2. \begin{cases} (5p+2) \times (5n+1) \mp 5qu^4 = w^4 \doteq 5n \pm 2, \\ (5p+3) \times (5n+1) \mp 5qu^4 = w^4 \doteq 5n \pm 3, \\ (5p+4) \times (5n+1) + 5qu^4 = w^4 \doteq 5n + 4. \end{cases}$$

Now, in the first set of these equations, in which it is supposed that $t^4 \mp 5n$, we have evidently, also, $w^4 \mp 5n'$, whereas it has been seen, that t^4, u^4, and w^4, are prime to each other; therefore, the equations are impossible, when $t^4 \mp 5n$.

Also, in the second set of equations, in which $t^4 \mp 5n+1$, we have

$$\begin{cases} w^4 \mp 5n \pm 2, \\ w^4 \mp 5n \pm 3, \\ w^4 \mp 5n + 4; \end{cases}$$

which are all impossible forms for 4th powers (cor. 2, art. 71). Therefore the equations

$$\begin{cases} (5p+2)t^4 \mp 5qu^4 = w^4, \\ (5p+3)t^4 \mp 5qu^4 = w^4, \\ (5p+4)t^4 + 5qu^4 = w^4, \end{cases}$$

are impossible, either in integers or fractions.

Q. E. D.

PROP. XVI.

75. The general indeterminate equations

$$(16p+r\ )t^4 + 2u^4 = w^4,$$
$$(16p+r'\ )t^4 + 3u^4 = w^4,$$
$$(16p+r'')t^4 + 4u^4 = w^4,$$
$$\&c. \qquad \&c. \qquad \&c.$$

are impossible, r being any number >1 and less than 14; that is, $r<14$, $r'<13$, $r''<12$, &c.

For t^4, u^4, and w^4, being prime to each other, and all 4th powers, being of one of the forms $16n$ or $16n+1$ (cor. 4, art. 71), it follows, that either t^4 and u^4 are each of the form $16n+1$, or one of them is of this form and the other of the form $16n$; which suppositions furnish the following cases:

1st, $t^4 \doteq 16n+1$, and $u^4 \doteq 16n'+1$. Then

$$1. \begin{cases} \begin{cases} (16p+r\ ) \times (16p+1) + 2(16n'+1) = w^4 \doteq \\ \quad 16n''+r+2, \end{cases} \\ \begin{cases} (16p+r'\ ) \times (16p+1) + 3(16n'+1) = w^4 \doteq \\ \quad 16n''+r'+3, \end{cases} \\ \begin{cases} (16p+r'') \times (16p+1) + 4(16n'+1) = w^4 \doteq \\ \quad 16n''+r''+4. \end{cases} \end{cases}$$

&c. &c. &c.

2d, $t^4 \doteq 16n$, and $u^2 \doteq 16n'+1$. Then

$$2. \begin{cases} (16p+r\ ) \times 16n + 2(16n'+1) = w^4 \doteq 16n''+2, \\ (16p+r'\ ) \times 16n + 3(16n'+1) = w^4 \doteq 16n''+3, \\ (16p+r'') \times 16n + 4(16n'+1) = w^4 \doteq 16n''+4. \end{cases}$$

3d, $t^4 \doteq 16n+1$, and $u^4 \doteq 16n$. Then

$$3. \begin{cases} (16p+r\ ) \times (16n+1) + 16n' = w^4 \doteq 16n''+r\ ; \\ (16p+r'\ ) \times (16n+1) + 16n' = w^4 \doteq 16n''+r'\ ; \\ (16p+r'') \times (16n+1) + 16n' = w^4 \doteq 16n''+r''. \end{cases}$$

Now, in the first set of these equations, we have $16n''+r+2$, $16n''+r'+3$, $16n+r''+4$; and since $r<14$, $r'<13$, $r''<12$, it is evident, that each of these forms $=16n+$, some quantity greater than 1, and less than 16; and, therefore, they are all impossible forms, by the converse of cor. 4, art. 71.

And the second set of these equations are evidently impossible, as are also the third; because r, r', r'', &c., are each >1, but <16. And, consequently, all the equations in these forms are impossible. — Q. E. D.

Scholium. The above set of forms furnishes an infinite number of impossible formulæ for biquadrates, or 4th powers, and various others might have been found; but as all those given for squares are equally applicable to 4th powers, it would be useless

to multiply them by other particular cases, as the methods which have been explained, the reader will easily apply to any particular case that may occur; and as he is thus furnished with so many cases of the impossibility of equations of the forms

$$ax^2 \pm by^2 = z^2, \ ax^3 \pm by^3 = z^3, \text{ and } ax^4 \pm by^4 = z^4,$$

which might have been carried to a much greater extent; it will always be proper, when any equations of these forms are proposed, to examine, first, whether they be possible or impossible; as, in the latter case, much unnecessary labour will be avoided. But it may be necessary to caution the young practitioner, that though an equation may fall under a possible form to one modulus, it may be impossible under another; and, therefore, that it is not so easy to show that an equation is possible, when it really is so, as to show the impossibility in those cases that are impossible. In short, there are no means of showing that an equation, which exceeds the 2*d* degree, is possible, but by solving it; but the impossibility may be frequently demonstrated by the methods above taught.

PROP. XVII.

76. No triangular number, except unity, is a biquadrate.

For, if possible, let

$$\frac{x(x+1)}{2} = y^4, \text{ or } x(x+1) = 2y^4;$$

now, since the two factors x and $x+1$ differ from each other only by unity, they are necessarily prime to each other: but if $2y^4$ be resolved into two

factors prime to each other, they must be $2m^4 \times n^4$; for it cannot be otherwise resolved into factors, that are prime to each other, and this leads to the following equations:

1st, $\begin{cases} x = 2m^4, \\ x+1 = n^4. \end{cases}$ 2d, $\begin{cases} x = n^4, \\ x+1 = 2m^4. \end{cases}$

The first gives $n^4 - 2m^4 = 1$, and the second

$$2m^4 - n^4 = 1.$$

The latter of these equations, by transposition, becomes $1 + n^4 = 2m^4$, which is impossible (cor. 2, art. 57); and, from the first, we derive

$$m^8 + n^4 = (m^4+1)^2, \text{ or } (m^2)^4 + n^4 = (m^4+1)^2,$$

which equation is also impossible (art. 58); therefore, no triangular number, except 1, is a biquadrate.

PROP. XVIII.

77. The 4th differences of consecutive 4th powers are constant, and equal to

$$1 \times 2 \times 3 \times 4 = 24.$$

For let $x-2$, $x-1$, x, $x+1$, $x+2$, represent the roots of any five consecutive 4th powers; then

$$\begin{aligned}
(x+2)^4 &= x^4 + 8x^3 + 24x^2 + 32x + 16, \\
(x+1)^4 &= x^4 + 4x^3 + 6x^2 + 4x + 1, \\
(x+0)^4 &= x^4, \\
(x-1)^4 &= x^4 - 4x^3 + 6x^2 - 4x + 1, \\
(x-2)^4 &= x^4 - 8x^3 + 24x^2 - 32x + 16.
\end{aligned}$$

$$\text{1st diff.} \begin{cases} 4x^3 + 18x^2 + 28x + 15, \\ 4x^3 + 6x^2 + 4x + 1, \\ 4x^3 - 6x^2 + 4x - 1, \\ 4x^3 - 18x^2 + 28x - 15. \end{cases}$$

$$\text{2d diff.} \begin{cases} 12x^2 + 24x + 14, \\ 12x^2 + 0x + 2, \\ 12x^2 - 24x + 14. \end{cases}$$

$$\text{3d diff.} \begin{cases} 24x + 12, \\ 24x - 12. \end{cases}$$

$$\text{4th diff.} = 24 = 1 \, . \, 2 \, . \, 3 \, . \, 4.$$

And if the common difference of their roots be d, then the 4th differences will be $1 \, . \, 2 \, . \, 3 \, . \, 4 \, . \, d^4$.

Q. E. D.

PROP. XIX.

78. Every 5th power is terminated with the same digit as its root. Or all 5th powers are of the same form, with regard to modulus 10, as the roots of those powers.

For all numbers to modulus 10 are of one of the following forms:

$$\begin{aligned}
(10n\phantom{{}+1})^5 &\doteqdot 10^5 n'^5 && \doteqdot 10n'', \\
(10n+1)^5 &\doteqdot 10n' + 1 && \doteqdot 10n'' + 1, \\
(10n+2)^5 &\doteqdot 10n' + 2^5 && \doteqdot 10n'' + 2, \\
(10n+3)^5 &\doteqdot 10n' + 3^5 && \doteqdot 10n'' + 3, \\
(10n+4)^5 &\doteqdot 10n' + 4^5 && \doteqdot 10n'' + 4, \\
(10n+5)^5 &\doteqdot 10n' + 5^5 && \doteqdot 10n'' + 5, \\
(10n+6)^5 &\doteqdot 10n' + 6^5 && \doteqdot 10n'' + 6, \\
(10n+7)^5 &\doteqdot 10n' + 7^5 && \doteqdot 10n'' + 7, \\
(10n+8)^5 &\doteqdot 10n' + 8^5 && \doteqdot 10n'' + 8, \\
(10n+9)^5 &\doteqdot 10n' + 9^5 && \doteqdot 10n'' + 9.
\end{aligned}$$

Where the latter formulæ are evidently the same as the first; and, consequently, the powers have the same forms to modulus 10 as the roots of those powers, or they are terminated with the same digits. — Q. E. D.

Cor. It has been demonstrated (art. 64), that all cubes have the same forms as their roots to modulus 6; and, in the above proposition, that all 5th powers have the same forms as their roots to modulus 10; and the same is universally true for prime powers; namely, that they are of the same form as their roots to modulus double the exponent of the power; *viz.* all 7th powers are of the same form as their roots to modulus 14, and 11th powers of the same form as their roots to modulus 22: and so on for any other prime powers,

PROP. XX.

79. The 5th differences of consecutive 5th powers are constant, and equal to

$$1 . 2 . 3 . 4 . 5 = 120.$$

For let $x-2$, $x-1$, x, $x+1$, $x+2$, $x+3$, represent the roots of any six consecutive 5th powers, then

$$\begin{aligned}
(x+3)^5 &= x^5 + 15x^4 + 90x^3 + 270x^2 + 405x + 243,\\
(x+2)^5 &= x^5 + 10x^4 + 40x^3 + 80x^2 + 80x + 32,\\
(x+1)^5 &= x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1,\\
(x+0)^5 &= x^5,\\
(x-1)^5 &= x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 1,\\
(x-2)^5 &= x^5 - 10x^4 + 40x^3 - 80x^2 + 80x - 32.
\end{aligned}$$

$$\text{1st diff.} \left\{ \begin{aligned}
&5x^4 + 50x^3 + 190x^2 + 325x + 211,\\
&5x^4 + 30x^3 + 70x^2 + 75x + 31,\\
&5x^4 + 10x^3 + 10x^2 + 5x + 1,\\
&5x^4 - 10x^3 + 10x^2 - 5x + 1,\\
&5x^4 - 30x^3 + 70x^2 - 75x + 31.
\end{aligned} \right.$$

$$\text{2d diff.}\left\{\begin{array}{l} 20x^3+120x^2+250x+180, \\ 20x^3+\ \ 60x^2+\ \ 70x+\ \ 30, \\ 20x^3+\ \ \ \ 0x^2+\ \ 10x+\ \ \ \ 0, \\ 20x^3-\ \ 60x^2+\ \ 70x-\ \ 30. \end{array}\right.$$

$$\text{3d diff.}\left\{\begin{array}{l} 60x^2+180x+150, \\ 60x^2+\ \ 60x+\ \ 30, \\ 60x^2-\ \ 60x+\ \ 30. \end{array}\right.$$

$$\text{4th diff.}\left\{\begin{array}{l} 120x+120, \\ 120x+\ \ \ \ 0. \end{array}\right.$$

$$\text{5th diff.} = 120 = 1 \,.\, 2 \,.\, 3 \,.\, 4 \,.\, 5.$$

Q. E. D.

And if the roots of any set of 5th powers form an arithmetical progression, the common difference of which is d, then will their 5th differences be equal to $1 \,.\, 2 \,.\, 3 \,.\, 4 \,.\, 5 \,.\, d^5$.

Scholium. It is also undoubtedly true, that the *nth* differences of consecutive *nth* powers are constant, and equal to $1 \,.\, 2 \,.\, 3 \,.\, 4 \,.\, 5 \,.\, 6$, &c. n; but it is difficult to demonstrate this on pure elementary principles. The demonstration appears to rest on the following theorem; *viz.* the product

$$1 \,.\, 2 \,.\, 3 \,.\, 4 \,.\, 5, \text{ - - - } n =$$

$$n^n - n(n-1)^n + \frac{n(n-1)}{1 \,.\, 2}(n-2)^n - \frac{n(n-1)(n-2)}{1 \,.\, 2 \,.\, 3}(n-3)^n + \text{ \&c.}$$

which is readily deduced from the *Differential Calculus*; but a demonstration, founded on those principles, could not, with propriety, be introduced into an elementary work of this kind.

CHAP. VI.

On the Properties of Powers in General.

PROP. I.

80. The difference of any two equal powers, of different numbers, is divisible by the difference of their roots; that is,

$$x^n - y^n = \text{M}(x-y)\,*.$$

For make $x-y=d$, or $x=d+y$; then x^n-y^n becomes $(d+y)^n-y^n$; and we have to demonstrate, that this expression is always divisible by d, or $x-y$.

Now, by the developement of $(d+y)^n$, and writing for the coefficients of the respective terms,

1, n, m, p, &c., n, 1, we have

$$(d+y)^n - y^n =$$
$$d^n + nd^{n-1}y + md^{n-2}y^2 + pd^{n-3}y^3 + \text{ - - - } ndy^{n-1} =$$
$$d(d^{n-1} + nd^{n-2}y + md^{n-3}y^2 + pd^{n-4}y^3 + \text{ - - - } ny^{n-1}),$$

which latter form is evidently divisible by d; and, consequently, the equal quantity

$$(d+y)^n - y^n, \text{ or } x^n - y^n$$

* The abridged expression $\text{M}(x-y)$ indicates a multiple of the quantity within the parentheses, and may be read either *x^n-y^n equal a multiple of $x-y$*; or *x^n-y^n divisible by $x-y$.*

is divisible also by d, or by $x-y$, since $x-y=d$; that is,

$$x^n-y^n=\mathrm{M}(x-y). \qquad \text{Q. E. D.}$$

Cor. 1. When x is prime to y, then $d=x-y$ is prime to both x and y (cor. 1, art. 7); and, consequently, the above quotient

$$d^{n-1}+nd^{n-2}y+md^{n-3}y^2+pd^{n-4}y^3+\ ---\ ny^{n-1}=$$
$$d(d^{n-2}+nd^{n-3}y+md^{n-4}y^2+pd^{n-5}y^3+\ ---)+ny^{n-1}$$

is prime to d, unless the power n be equal to d, or some multiple of d; for all the terms, except the last, are divisible by d; but the last ny^{n-1} is prime to d, unless n be a multiple of it; because we have seen that d is prime to y, and, therefore, the quotient is not divisible by d, except in the latter case; and hence we conclude, that x^n-y^n is always divisible by $x-y$ *once*, but after that, the quotient is not again divisible by $x-y$, unless $n=x-y$, or $n=$ some multiple of $x-y$.

Cor. 2. If n be a prime number, then the coefficients of the expanded binomial $d+y$ may be represented by

1, n, na, nb, &c., nb, na, n, 1 (cor. 1, art. 12),

in which case

$$(d+y)^n-y^n \text{ becomes}$$

$$\left\{\begin{array}{l} d^n+nd^{n-1}y+nad^{n-2}y^2+nbd^{n-3}y^3,\ ---\ nad^2y^{n-2}+ \\ \qquad ndy^{n-1}= \end{array}\right.$$

$$\left\{\begin{array}{l} d(d^{n-1}+nd^{n-2}y+nad^{n-3}y^2+nbd^{n-4}y^3,\ ---\ nady^{n-2} \\ \qquad +ny^{n-1}), \end{array}\right.$$

which, being divided by d, gives for a quotient

$$\left\{\begin{array}{l} d(d^{n-2}+nd^{n-3}y+nad^{n-4}y^2+nbd^{n-5}y^3,\ ---\ nay^{n-2}) \\ \qquad +ny^{n-1}, \end{array}\right.$$

which is evidently not again divisible by d, unless $n=d$; for since n is a prime, it cannot be a multiple of d. But this quotient may be divisible by n, if n be a factor of d; for if we make $d=nd'$, the above becomes

$$\begin{cases} nd'\{(nd')^{n-2}+n(nd')^{n-3}y+na(nd')^{n-4}y^3+ \ \cdots \\ \quad nay^{n-2}\}+ny^{n-1}, \end{cases}$$

which is evidently divisible by n, giving for a quotient

$$\begin{cases} d'\{(nd')^{n-2}+n(nd')^{n-3}y+na(nd')^{n-4}y^3+ \ \cdots \\ \quad nay^{n-2}\}+y^{n-1}; \end{cases}$$

but this quotient is not again divisible by n; for, since n is a factor of d, and d is prime to y, y^{n-1} is prime to n; and, since all the first part of this quotient is divisible by n, but the other part, y^{n-1}, is prime to n; therefore, the whole quotient is also prime to n. And hence we conclude, that the difference of two powers, x^n-y^n (when x and y are prime to each other, and n is a prime number) can only be divided *once* by $x-y$; and after that, neither by $x-y$ nor by any factor of $x-y$, unless $n=x-y$, or some factor of $x-y$; in which case, x^n-y^n is divisible *once* by $n(x-y)$, but after that, neither by n nor by $(x-y)$, nor by any factor of $x-y$.

Cor. 3. The quotient really arising from the division x^n-y^n by $x-y$ is

$$\begin{cases} \dfrac{x^n-y^n}{x-y}=x^{n-1}+x^{n-2}y+x^{n-3}y^2+x^{n-4}y^3+ \ \cdots \ xy^{n-2} \\ \quad +y^{n-1}, \end{cases}$$

which quotient, therefore, from what has been shown above, is always prime to $x-y$ (x and y being

supposed prime to each other); except when n is equal to $x-y$, or when it is some multiple or factor of $x-y$.

PROP. II.

81. The difference of two equal powers is always divisible by the sum of their roots, when the exponent of the power is an even number; that is, $x^n - y^n = \text{M}(x+y)$, when n is even.

For make $x+y=s$, or $x=s-y$, then $x^n - y^n$ becomes $(s-y)^n - y^n$, which we have to prove is always divisible by $x+y$ or s.

Now by the developement of $(x+y)^n$, and writing for the coefficients of this expanded binomial,

$$1, \; n, \; m, \; p, \; \&\text{c.}, \; m, \; n, \; 1,$$

it becomes

$$(s-y)^n - y^n =$$

$$\begin{cases} s^n - ns^{n-1}y + ms^{n-2}y^2 - ps^{n-3}y^3 + \; - - - \; + ms^2y^{n-2} - \\ \quad nsy^{n-1}; \end{cases}$$

because, since n is even, the last term of $(s-y)^n$, namely y^n, will have the sign $+$, and will, therefore, be cancelled by $-y^n$.

Now this quantity may be put under the form

$$\begin{cases} s(s^{n-1} - ns^{n-2}y + ms^{n-3}y^2 - ps^{n-4}y^3 + \; - - - \; + msy^{n-2} \\ \quad - ny^{n-1}), \end{cases}$$

which is evidently divisible by s; and, consequently, the equal quantity $(s-y)^n - y^n$, or $x^n - y^n$ is also divisible by s, or by $x+y$; that is,

$$x^n - y^n = \text{M}(x+y),$$

when n is an even number. — Q. E. D.

Cor. It may also be demonstrated, by the same reasoning as that employed above (cor. 1, art. 80),

that, if x and y be prime to each other, then $x^n - y^n$ can only be divided once by $x+y$, unless n be equal to $x+y$, or some multiple of $x+y$.

PROP. III.

82. The sum of two equal odd powers is always divisible by the sum of their roots; that is,

$$x^n + y^n = \text{M}(x+y),$$

when the exponent n is an odd number.

For make $x+y=s$, or $x=s-y$, then x^n+y^n becomes $(s-y)^n+y^n$; which we have to demonstrate is always divisible by s, or $x+y$.

Now by the developement of $(s-y)^n$, and writing

$$1,\ n,\ m,\ p,\ \&\text{c.},\ m,\ n,\ 1,$$

for the coefficients of the expanded binomial $(s-y)^n$, we have

$$(s-y)^n + y^n =$$

$$\left\{\begin{array}{l} s^n - ns^{n-1}y + ms^{n-2}y^2 - ps^{n-3}y^3 + \ --- \ + ms^2y^{n-2} - \\ \quad nsy^{n-1}, \end{array}\right.$$

for since n is odd, the last term of the expanded binomial $(s-y)^n$, or y^n, will have the sign $-$, and will, therefore, be cancelled by $+y^n$.

And this expression may be put under the form

$$\left\{\begin{array}{l} s(s^{n-1} - ns^{n-2}y + ms^{n-3}y^2 - ps^{n-4}y^3 + \ --- \ + msy^{n-2} \\ \quad - ny^{n-1}), \end{array}\right.$$

which is evidently divisible by s; and, therefore, the equal quantity $(s-y)^n+y^n$, or x^n+y^n, is also divisible by s, or by $x+y$; that is,

$$x^n + y^n = \text{M}(x+y),$$

when n is an odd number. — Q. E. D.

Cor. 1. It may also be demonstrated, by the same

reasoning as that employed at cor. 1, art. 80, that if x and y be prime to each other, then $x^n + y^n$ can only be divided by $x+y$ *once*, unless $n = (x+d)$, or some multiple of $(x+d)$.

Cor. 2. And if n be a prime number, and x and y prime to each other, then $x^n + y^n$ can only be divided by $x+y$ *once*; and after that neither by $x+y$ nor by any factor of $x+y$, unless n be one of its factors, in which case it may be divisible by $n(x+y)$ *once*, but after that neither by n nor by $(x+y)$, nor by any factor of $(x+y)$; as is evident from the same reasoning as that employed at cor. 2, art. 80.

Scholium. By means of the three foregoing propositions, and their corollaries, we may draw the following general conclusion with regard to the divisors of the formula $x^n \pm y^n$; *viz.*

1. If n be even, or of the form $2n'$, then $(x^n - y^n)$,

$$\text{or } (x^{2n'} - y^{2n'}) = \text{M}(x+y); \text{ and } \text{M}(x-y).$$

But if x be prime to y then will $x^{2n'} - y^{2n'}$ be divisible only once, by each of those quantities, unless $2n' = x+y$, or $x-y$, or some multiple of one of those quantities.

2. If n be odd, or of the form $2n'+1$, then

$$(x^n - y^n), \text{ or } (x^{2n'+1} - y^{2n'+1}) = \text{M}(x-y); \text{ and}$$
$$(x^n + y^n), \text{ or } (x^{2n'+1} + y^{2n'+1}) = \text{M}(x+y).$$

But if in these formulæ x and y be prime to each other, then each of those quantities are only divisible by their respective divisors *once*, unless $2n'+1 = x-y$, or some multiple of $x-y$, in the first case; or $2n'+1 = x+y$, or some multiple of $x+y$, in the second case. And if in these two last forms,

x and y be prime to each other, and n be a prime number, then, in the first form, $x^n - y^n$ is divisible by $x - y$ *once*, and after that neither by $x - y$ nor by any factor of $(x - y)$, unless n be one of its factors; in which case $x^n - y^n$ is divisible $n(x - y)$ *once*, and after that neither by n nor by $(x - y)$, nor by any factor of $(x - y)$.

And in the second form, $(x^n + y^n)$ is divisible by $x + y$ once, and after that neither by $(x + y)$ nor by any factor of $x + y$, unless n be one of its factors; in which case it is divisible by $n(x + y)$ once, and after that neither by n nor by $(x + y)$, nor by any factor of $x + y$.

By means of the above propositions, we are also enabled to ascertain the divisors of the sum or difference of unequal powers of the same root; *viz.*

$$(x^m - x^n) = \text{M}(x - 1), \text{ and } \text{M}(x + 1),$$

when $m - n$ is even, or of the form $2n'$, for

$$x^m - x^n = x^n \times (x^{m-n} - 1),$$

and since $m - n \doteq 2n'$, therefore,

$$(x^{m-n} - 1) = (x^{2n} - 1^{2n}) = \text{M}(x - 1), \text{ and } \text{M}(x + 1);$$

and, consequently,

$$x^n \times (x^{m-n} - 1) = (x^m - x^n) = \text{M}(x - 1), \text{ and } \text{M}(x + 1).$$

Again, if $n - m$ be odd, or of the form $2n' + 1$, then

$$(x^m - x^n) = \text{M}(x - 1), \text{ and}$$
$$(x^m + x^n) = \text{M}(x + 1).$$

For

$$(x^m - x^n) = x^n \times (x^{m-n} - 1), \text{ and}$$
$$(x^m + x^n) = x^n \times (x^{m-n} + 1);$$

also, since $m - n \doteq 2n' + 1$, therefore,

$$(x^{m-n}-1)=(x^{2n+1}-1^{2n+1})=\text{M}(x-1),\text{ and}$$
$$(x^{m-n}+1)=(x^{2n+1}+1^{2n+1})=\text{M}(x+1);$$

and, consequently,

$$x^n \times (x^{m-n}-1)=(x^m-x^n)=\text{M}(x-1),$$
$$x^n \times (x^{m-n}+1)=(x^m+x^n)=\text{M}(x+1).$$

Lemma.

83. In demonstrating the impossibility of the equation $x^n \pm y^n = z^n$, it will be sufficient to consider n as a prime number. For suppose n be not a prime, but equal to the product of two or more prime factors, as $n=pq$, then the equation becomes

$$x^{pq} \pm y^{pq} = z^{pq} = (x^p)^q \pm (y^p)^q = (z^p)^q,$$

being a similar equation, in which the power q is a prime number; and, therefore, if the equation be possible when n is a composite number, it is also possible for a prime power; and, conversely, if the equation be impossible when the power is a prime, it is also impossible for every composite power; we shall, therefore, in what follows, consider n as a prime number.

Again, we may always suppose x, y, and z, as prime to each other; for it is evident, in the first place, that two of these numbers cannot contain a common divisor, unless the third contains the same. Suppose, for example, that x^n and y^n contained any common divisor, as ϕ, and that z^n did not contain the same, then, in the equation $x^n \pm y^n = z^n$, we should have $x^n \pm y^n$ divisible by ϕ, but the equal quantity z^n not divisible by it, which is absurd; and the same may be shown if any other two of these quantities are supposed to have a common

divisor which the third has not. And if they have all three the same common divisor, as $x=\phi x'$, $y=\phi y'$, and $z=\phi z'$, then the equation becomes

$$\phi^n x'^n \pm \phi^n y'^n = \phi^n z'^n,$$

or, dividing by the greatest common divisor,

$$x'^n \pm y'^n = z'^n:$$

if, therefore, the equation $x^n \pm y^n = z^n$ be possible, when x, y, and z, have a common divisor, it is also possible after being divided by that common divisor, and in which latter equation the three resulting quantities, x', y', and z', are prime to each other; and, conversely, if the latter be impossible, the former is impossible also; we shall, therefore, only consider the cases in which x, y, and z, are prime amongst themselves.

It will also be sufficient to consider the ambiguous sign $\pm$ under either of its forms $+$ or $-$; for if the equation $x^n + y^n = z^n$ be possible, so also is the equation $z^n - y^n = x^n$; and if the equation be impossible under the latter form, it is likewise impossible under the former.

We shall therefore limit our demonstration to the equation $x^n - y^n = z^n$, in which n is a prme number, and x, y, and z, numbers prime to each other; the impossibility of which, from what is said above, involves with it the impossibility of the general equation $x^n \pm y^n = z^n$, when x, y, and z, are any numbers whatever, and n any number except 2, or some power of 2. Now, with regard to $n=2$, we know, that the equation is not impossible, but the case of n equal 4 has been demonstrated to

be impossible (art. 73); and this latter case involves that of every higher power of 2, thus

$$x^8 \pm y^8 = z^8 = (x^2)^4 \pm (y^2)^4 = (z^2)^4,$$

which being impossible in the latter form, is necessarily so in the former; and, in the same manner, the impossibility of the equation for any higher power of 2 may be shown to be involved in that of $n=4$: it is evident, therefore, that our equation, together with that of $n=4$, involves every possible value of n greater than 2.

PROP. IV.

84. If the equation $x^n - y^n = z^n$ be possible (n being a prime number, and x, y, and z, prime to each other), then one of the four following conditions must obtain; *viz.*,

$$\text{1st,} \begin{cases} x-y \doteq r^n, \\ x-z \doteq s^n, \\ y+z \doteq t^n. \end{cases} \qquad \text{2d,} \begin{cases} x-y \doteq n^{n-1}r^n, \\ x-z \doteq s^n, \\ y+z \doteq t^n. \end{cases}$$

$$\text{3d,} \begin{cases} x-y \doteq r^n, \\ x-z \doteq n^{n-1}s^n, \\ y+z \doteq t^n. \end{cases} \qquad \text{4th,} \begin{cases} x-y \doteq r^n, \\ x-z \doteq s^n, \\ y+z \doteq n^{n-1}t^n. \end{cases}$$

Where r, s, and t, may represent any numbers whatever, indicating only, that $(x-y)$, $(x-z)$, $(y+z)$, &c., are complete *nth* powers, or that they are of the form r^n, s^n, t^n. This follows from what has been demonstrated cor. 2, art. 80; *viz.* that $x^n - y^n$ is divisible by $x-y$ once, and after that neither by $x-y$ nor by any factor of $x-y$, unless n be one of its factors, in which case $x^n - y^n$ is divisible by $n(x-y)$ once, and after that neither by n nor by $x-y$, nor by any

factor of $x-y$; and the same must necessarily be true of the equal quantity z^n; *viz.* that it is divisible by $x-y$ once, or by $n(x-y)$ once, when n is a factor of $x-y$, but after that it is neither divisible by n nor by $x-y$, nor by any factor of $x-y$, and, therefore, (cor. 1, art. 16) $x-y$, in the first case, and $n(x-y)$ in the second, must be complete *nth* powers; that is,

$$x-y \doteqdot r^n, \text{ or } n(x-y) \doteqdot rn;$$

but the latter of these forms, since n is a prime number, must be

$$n(x-y) \doteqdot n^n r'^n, \text{ or } x-y \doteqdot n^{n-1} r'^n;$$

and, consequently, if the equation

$$x^n - y^n = z^n$$

be possible, we must have $x-y \doteqdot r^n$, or $n^{n-1}r^n$.

But the equation $x^n - y^n = z^n$ may be put under the form $x^n - z^n = y^n$; and, consequently, we have also the same result as to the difference $x-z$; *viz.*

$$x-z \doteqdot s^n, \text{ or } n^{n-1}s^n.$$

And again, by writing the equation thus,

$$y^n + z^n = x^n,$$

we shall, by means of cor. 2, art. 82, and the same reasoning as that employed above, find, that

$$y+z \doteqdot t^n, \text{ or } n^{n-1}t^n.$$

Hence, then, if the equation

$$x^n - y^n = z^n$$

be possible, the following conditions must obtain; *viz.*

The difference of the roots $x-y \doteqdot r^n$, or $n^{n-1}r^n$.

The difference of the roots $x-z \doteqdot s^n$, or $n^{n-1}s^n$.

The sum of the roots $y+z \doteqdot t^n$, or $n^{n-1}t^n$.

But since $(x-y)$, $(x-z)$, and $(y+z)$, are respectively divisors of the three *nth* powers, z^n, y^n, and x^n, and since these three quantities are prime to each other, their divisors must also be prime to each other; and, consequently, only one of these can be of the latter form above given, as they would otherwise have a common divisor n. Therefore, if the equation be possible, we shall have either

$$\begin{cases} x-y \mp r^n, \\ x-z \mp s^n, \\ y+z \mp t^n, \end{cases}$$

or two of these quantities will be of this form, and the third of the form $n^{n-1}\phi^n$, which evidently resolves into the four following cases, one of which must necessarily obtain, if the equation $x^n - y^n = z^n$ be possible; *viz.*

$$\text{1st}, \begin{cases} x-y \mp r^n, \\ x-z \mp s^n, \\ y+z \mp t^n. \end{cases} \qquad \text{2d}, \begin{cases} x-y \mp n^{n-1}r^n, \\ x-z \mp s^n, \\ y+z \mp t^n. \end{cases}$$

$$\text{3d}, \begin{cases} x-y \mp r^n, \\ x-z \mp n^{n-1}s^n, \\ y+z \mp t^n. \end{cases} \qquad \text{4th}, \begin{cases} x-y \mp r^n, \\ x-z \mp s^n, \\ y+z \mp n^{n-1}t^n. \end{cases}$$

Q. E. D.

PROP. V.

85. The equation $x^n - y^n = z^n$ is impossibl[e] in integers, n being any prime number greate[r] than 2.

We have before observed that x, y, and z, ma[y] be considered as prime to each other, and by th[e] foregoing proposition it is demonstrated, that, if th[e] equation be possible, one of the four followin[g] conditions must obtain; *viz.*

1st, $\begin{cases} x-y=r^n,\text{*} \\ x-z=s^n, \\ y+z=t^n. \end{cases}$ 2d, $\begin{cases} x-y=n^{n-1}r^n, \\ x-z=s^n, \\ y+z=t^n. \end{cases}$

3d, $\begin{cases} x-y=r^n, \\ x-z=n^{n-1}s^n, \\ y+z=t^n. \end{cases}$ 4th, $\begin{cases} x-y=r^n, \\ x-z=s^n, \\ y+z=n^{n-1}t^n. \end{cases}$

But at present we shall only consider one of those cases, for example the first, and in the result, by substituting $n^{n-1}r^n$ for r^n, $n^{n-1}s^n$ for s^n, &c., we shall arrive at all the possible cases. First then, let us ascertain whether the equation $x^n-y^n=z^n$ be possible, on the supposition that

$$x-y=r^n,$$
$$x-z=s^n,$$
$$y+z=t^n.$$

Now from these three equations we derive the three following; *viz.*

$$x=\tfrac{1}{2}\{t^n+(s^n+r^n)\},$$
$$y=\tfrac{1}{2}\{t^n+(s^n-r^n)\},$$
$$z=\tfrac{1}{2}\{t^n-(s^n-r^n)\}.$$

And, consequently, since $x^n-y^n=z^n$, or $x^n=y^n+z^n$, we have

$$\left(\frac{t^n+(s^n+r^n)}{2}\right)^n=\left(\frac{t^n-(s^n-r^n)}{2}\right)^n+\left(\frac{t^n+(s^n-r^n)}{2}\right)^n.$$

Or

$$\{t^n+(s^n+r^n)\}^n=\{t^n-(s^n-r^n)\}^n+\{t^n+(s^n-r^n)\}^n.$$

Now

$$\left\{ \begin{array}{l} \{t^n+(s^n-r^n)\}^n=t^{nn}+nt^{nn-n}(s^n-r^n)+nat^{nn-2n}(s^n- \\ \quad r^n)^2+nbt^{nn-3n}(s^n-r^n)^3 \text{ \&c.} \end{array} \right.$$

* See note, page 137.

$$\left\{ \begin{array}{l} \{t^n - (s^n - r^n)\}^n = t^{nn} - nt^{nn-n}(s^n - r^n) + nat^{nn-2n}(s^n - \\ \quad r^n)^2 - nbt^{nn-3n}(s^n - r^n)^3 + \&c. \end{array} \right.$$

$$\left\{ \begin{array}{l} \{t^n + (s^n + r^n)\}^n = t^{nn} + nt^{nn-n}(s^n + r^n) + nat^{nn-2n}(s^n + \\ \quad r^n)^2 + nbt^{nn-3n}(s^n + r^n)^3 - \&c.* \end{array} \right.$$

And here, since the sum of the two first expressions is equal to the third, it is evident that the latter, subtracted from the sum of the two former, is equal to zero. But in adding the two first together, the 2d, 4th, &c., terms cancel; and, consequently, in subtracting the latter from that sum, the 2d, 4th, &c., terms will remain the same, except that the signs will be changed from + to −. And as to the 1st, 3d, &c., terms of the first two equations, and the same terms of the third, we shall have, by observing that

$$(s^n - r^n)^2 = (s^n + r^n)^2 - 4s^n r^n,$$
$$(s^n - r^n)^4 = (s^n + r^n)^4 - 8(s^{3n}r^n + s^n r^{3n}),$$
$$(s^n - r^n)^6 = (s^n + r^n)^6 - 12s^{5n}r^n - 40s^{3n}r^{3n} - 12s^n r^{5n},$$
$$\&c. \qquad \&c. \qquad \&c.$$

for the sum of the two

1st terms $2t^{nn}$,

3d terms $2nat^{nn-2n}(s^n + r^n)^2 - 2nat^{nn-2n} \times 4s^n r^n$,

5th terms $2nct^{nn-4n}(s^n + r^n)^4 - 2nct^{nn-4n} \times 8s^n r^n(s^{2n} + r^{2n})$,

7th terms, &c.

And, consequently, subtracting from those sums the 1st, 3d, &c., terms of the third line, namely,

1st term t^{nn},

3d term $nat^{nn-2n}(s^n + r^n)^2$,

5th term $nct^{nn-4n}(s^n + r^n)^4$;

the remainders of these particular terms will be,

* By writing *n, na, nb, nc,* &c., for the coefficients of the binomial, cor. 1, art. 12.

1st rem. $= t^{nn}$,

3d rem. $= nat^{nn-2n}(s^n + r^n)^2 - 2nat^{nn-2n} \times 4s^n r^n$,

5th rem. $= nct^{nn-4n}(s^n + r^n)^4 - 2nct^{nn-4n} \times 8s^n r^n (s^{2n} + r^{2n})$,

7th rem. &c. &c.

In short, the whole of the remainder which is equal to zero, will be expressed by

$$\{t^n - (s^n + r^n)\}^n - (2nat^{nn-2n}.4s^n r^n) - (2nct^{nn-4n}.8s^n r^n)(s^{2n} + r^{2n}) - \text{ \&c.}$$

And here it is only necessary to observe, that all the terms on the latter side of this expression are divisible by $t^n s^n r^n$, so that, for perspicuity sake, we may write it thus,

$$\{t^n - (s^n + r^n)\}^n - t^n s^n r^n \text{A} = 0;$$

and, consequently,

$$\{t^n - (s^n + r^n)\}^n = t^n s^n r^n \text{A};$$

and here, since the first side is a complete *nth* power, the latter side, which is equal to it, must be so likewise; and, consequently, A must be a complete *nth* power, or $\text{A} = \text{A}'^n$; that is,

$$\{t^n - (s^n + r^n)\}^n = t^n s^n r^n \text{A}'^n;$$

and, therefore,

$$t^n - s^n - r^n = tsr\text{A}';$$

or, dividing by *trs*, we have

$$\frac{t^{n-1}}{sr} - \frac{s^{n-1}}{tr} - \frac{r^{n-1}}{st} = \text{A}',$$

which must necessarily be an integer. But these three fractions are in their lowest terms, because *r*, *s*, and *t*, are prime to each other, and

each of the denominators contains a factor that is not common to the other two; they cannot, therefore, be equal to an integer (cor. 2, art. 13); and, consequently, the equation is impossible under the first condition. And in order to arrive at the results of the other three conditions, we have only to substitute $n^{n-1}r^n$ for r^n; $n^{n-1}s^n$ for s^n; and $n^{n-1}t^n$ for t^n, whence we draw the four following conclusions;

$$\text{1st,}\quad \frac{t^{n-1}}{rs}-\frac{s^{n-1}}{tr}-\frac{r^{n-1}}{st}=\text{A}',$$

$$\text{2d,}\quad \frac{t^{n-1}}{rs}-\frac{s^{n-1}}{tr}-\frac{n^{n-1}r^{n-1}}{st}=\text{A}'',$$

$$\text{3d,}\quad \frac{t^{n-1}}{rs}-\frac{n^{n-1}s^{n-1}}{tr}-\frac{r^{n-1}}{st}=\text{A}''',$$

$$\text{4th,}\quad \frac{n^{n-1}t^{n-1}}{rs}-\frac{s^{n-1}}{tr}-\frac{r^{n-1}}{st}=\text{A}'''',$$

according as we assume the 1st, 2d, 3d, or 4th, condition. In which expressions we ought to have one of the quantities A′, A″, A‴, A⁗, an integer number, if the given equation were possible; but since in each of these expressions we have three fractions, in their lowest terms, and the denominator of each contains a factor not common to the other two, therefore (cor. 2, art. 13) they cannot produce an integer number.

Having shown, therefore, that, if the equation $x^n-y^n=z^n$ were possible, one of the quantities A′, A″, A‴, or A⁗, would be an integer; and having also demonstrated that no one of these quantities can be an integer; it follows, that the equation

whence they were derived is impossible; that is, the equation $x^n - y^n = z^n$ is impossible, when n is a prime number.

We have also demonstrated, art. 83, that the impossibility of the equation $x^n - y^n = z^n$, when n is a prime, involves with it the impossibility of every equation of the form

$$x^n \pm y^n = z^n,$$

in which n is any number whatever except 2, or some power of 2; and we have likewise shown that the impossibility of the equation, when n is any power of 2, is involved in that of $x^4 - y^4 = z^4$, which particular case has been demonstrated to be impossible (art. 73); and, consequently, the equation

$$x^n \pm y^n = z^n$$

is always impossible, when n is any integer number whatever greater than 2.—Q. E. D.

Cor. Since the equation

$$x^n \pm y^n = z^n$$

is impossible, so also is $\frac{x^n}{m^n} \pm \frac{y^n}{p^n} = \frac{z^n}{q^n}$, for this is the same as $x^n + y^n = \frac{z^n m^n p^n}{q^n}$: and, therefore, the equation is likewise impossible in fractions.

PROP. VI.

86. If m be a prime number and x any number not divisible by m, then will the remainder arising from the division of x by m be the same as that from the division of x^m by m.

For make $x=x'+1$, then we have

$$x^m=(x'+1)^m=x'^m+mx'^{m-1}+max'^{m-2}+ - - - mx+1.$$

And since all the terms of this expanded binomial, except the first and last, are divisible by m (cor. 1, art. 12), it follows that the remainder from the division $(x'+1)^m$ by m is the same as that from the division x'^m+1 by m; which, by rejecting the multiples of m, may be expressed thus:

$$x^m=(x'+1)^m=x'^m+1.$$

Making now $x'=x''+1$, we shall have, on the same principles,

$$x^m=(x'+1)^m=x'^m+1=(x''+1)^m+1=x''^m+2.$$

Again, let $x''=x'''+1$, and we obtain

$$x^m=x'^m+1=x''^m+2=x'''^m+3.$$

And thus, by continual substitutions, we have

$$x^m=x'^m+1=x''^m+2=x'''^m+3= \&c.; \text{ or,}$$

$$\begin{cases} x^m=(x-1)^m+1=(x-2)^m+2=(x-3)^m+3 \ \&c. \\ \quad (x-x)^m+x, \end{cases}$$

the last of which terms is equal to x; whence it follows, that the remainder arising from the division of x by m is the same as that from the division of x^m by m.—Q. E. D.

PROP. VII.

87. If m be a prime number, and x any number not divisible by m, then will the formula $x^{m-1}-1$ be divisible by m, or, which is the same,

$$(x^{m-1}-1)=\text{M}(m).$$

For, by the foregoing proposition, the remainder of $\frac{x}{m}$ is the same as the remainder of $\frac{x^m}{m}$; and, con-

sequently, the difference $x^m - x$ is divisible by m. But $x^m - x = x(x^{m-1} - 1)$, and since this product is divisible by m, and the factor x is prime to m, it must therefore be the other factor $(x^{m-1} - 1)$, that is divisible by m (cor. 5, art. 11). — Q. E. D.

Cor. 1. Since $x^{m-1} - 1$ is always divisible by m, if x be prime to m, and m itself a prime, there are, necessarily, $m - 1$ values of x less than m, that satisfy the equation

$$\frac{x^{m-1} - 1}{m} = e, \text{ an integer;}$$

that is, x may be any number in the series

$$1,\ 2,\ 3,\ 4,\ 5,\ \&c.,\ m - 1,$$

because all of these numbers are necessarily prime to m; and, since $m - 1$ is an even number, we shall have also $m - 1$ values of x, comprised between the limits $-\frac{1}{2}m$ and $\frac{1}{2}m$; that is, x may be any number in the series

$$\pm 1,\ \pm 2,\ \pm 3,\ \pm 4\ \text{- - -}\ \pm \frac{m-1}{2};$$

so that, in both cases, we have $m - 1$ values $x < m$, that render the equation

$$\frac{x^{m-1} - 1}{m} = e, \text{ an integer.}$$

Cor. 2. Since $x^{m-1} - 1$ is always divisible by m under the limitations of the proposition, therefore, $x^{m-1} = am + 1$; and, consequently, every power, whose exponent plus 1 is a prime number, as (m), will be of the form am, or $am + 1$; and thus we may ascertain the forms of many of the higher powers: thus,

$$x^4 \text{ ǂ } 5n, \text{ or } 5n+1;$$
$$x^6 \text{ ǂ } 7n, \text{ or } 7n+1;$$
$$x^{10} \text{ ǂ } 11n, \text{ or } 11n+1;$$
$$x^{12} \text{ ǂ } 13n, \text{ or } 13n+1;$$
&c. &c. &c.

Again, since m is a prime number, if it be greater than 2, it is an odd number; and, consequently, $m-1$ an even number; and, therefore,

$$x^{m-1}-1=\left(x^{\frac{m-1}{2}}+1\right)\times\left(x^{\frac{m-1}{2}}-1\right);$$

and, since this product,

$$\left(x^{\frac{m-1}{2}}+1\right)\times\left(x^{\frac{m-1}{2}}-1\right),$$

is divisible by m, and m is a prime number, one of these factors must be divisible by m; that is,

$$x^{\frac{m-1}{2}} \text{ ǂ } ma\pm1;$$

and, consequently, every power, the double of whose exponent plus 1 is a prime number, as (m), is of one of the forms

$$am, \text{ or } am\pm1;$$

and hence again, we derive the forms of many other higher powers; thus,

$$x^3 \text{ ǂ } 7n, \text{ or } 7n\pm1;$$
$$x^5 \text{ ǂ } 11n, \text{ or } 11n\pm1;$$
$$x^6 \text{ ǂ } 13n, \text{ or } 13n\pm1;$$
$$x^8 \text{ ǂ } 17n, \text{ or } 17n\pm1;$$
$$x^9 \text{ ǂ } 19n, \text{ or } 19n\pm1;$$
$$x^{11} \text{ ǂ } 23n, \text{ or } 23n\pm1;$$
&c. &c. &c.

And hence we have the following forms of all

powers from 2 to 12, the 7th powers only excepted, which cannot be introduced into these forms, because neither $7+1$, nor $2 \cdot 7+1$, is a prime number.

Table of the possible Forms of Powers, from 2 to 12.

$x^2 \neq$	$3n$, or $3n+1 \neq$	$5n$, or $5n \pm 1$;
$x^3 \neq$	- - - - $\neq$	$7n$, or $7n \pm 1$;
$x^4 \neq$	$5n$, or $5n+1 \neq$	- - - - -
$x^5 \neq$	- - - - $\neq$	$11n$, or $11n \pm 1$;
$x^6 \neq$	$7n$, or $7n+1 \neq$	$13n$, or $13n \pm 1$;
$x^7 \neq$	- - - - $\neq$	- - - - -
$x^8 \neq$	- - - - $\neq$	$17n$, or $17n \pm 1$;
$x^9 \neq$	- - - - $\neq$	$19n$, or $19n \pm 1$;
$x^{10} \neq$	$11n$, or $11n+1 \neq$	- - - - -
$x^{11} \neq$	- - - - $\neq$	$23n$, or $23n \pm 1$;
$x^{12} \neq$	$13n$, or $13n+1 \neq$	- - - - -

Scholium. By means of the foregoing table of formulæ, we may frequently satisfy ourselves of the possibility or impossibility of equations of the form

$$ax^n \pm by^n = dz^n.$$

And also whether any given number a is a complete power or not, without the trouble of extracting its root: it is to be observed, however, that a given number may be of a possible form, though it be not a complete power; but if it be of an impossible form, then we are certain, without any farther trouble, that it is not a complete power.

PROP. VIII.

88. If m be a prime number, and P be made to represent any polynomial of the nth degree, as

$$P = x^n + ax^{n-1} + bx^{n-2} + c^{n-3} + \text{ - - - } q,$$

then, I say, there cannot be more than n values of x, between the limits $+\frac{1}{2}m$, and $-\frac{1}{2}m$, that render this polynomial divisible by m.

For let k be the first value of x, that renders P divisible by m, so that

$$Am = k^n + ak^{n-1} + bk^{n-2} + ck^{n-3} + \text{ - - - } q;$$

then, by subtraction, we have

$$\left\{ \begin{array}{l} P - Am = (x^n - k^n) + a(x^{n-1} - k^{n-1}) + b(x^{n-2} - k^{n-2}) + \\ \quad \&c. \end{array} \right.$$

But the latter side of this equation, being divided by $x - k$ (art. 80), we shall have for a quotient a polynomial of the degree $n - 1$; which, being represented by P′, gives

$$P - Am = (x - k)P', \text{ or } P = (x - k)P' + Am.$$

Let now k' be a second value of x, that renders P divisible by m, then it follows, that $(x - k)P' + Am$ is also divisible by m; and, consequently, $(x - k)P'$ divisible by m, but the factor $x - k$, which now becomes $(k' - k)$, cannot be divisible by m, because both k' and k are less than $\frac{1}{2}m$; therefore, P cannot be divisible a second time by m, unless P′ be divisible by m.

The polynomial P is, therefore, only once more divisible by m than the polynomial P′; and, in the same manner, it may be shown, that P′, of the degree $n - 1$, is only once more divisible by m, than

P″, of the $n-2$ degree, &c.; and hence it follows, that, P being a polynomial of the n degree, there can be only n different values of x, comprised between the limits $+\frac{1}{2}m$ and $-\frac{1}{2}m$, that render it divisible by m. — Q. E. D.

Cor. We have seen (cor. 1, art. 87), that if m be a prime number, the formula $x^{m-1}-1$ has $m-1$ values of x, between the limits $+\frac{1}{2}m$ and $-\frac{1}{2}m$, that render it divisible by m. Now, this being put under the form $\left(x^{\frac{m-1}{2}}+1\right)\times\left(x^{\frac{m-1}{2}}-1\right)$, it follows, that each of these factors has $\frac{m-1}{2}$ values of x, between the limits $+\frac{1}{2}m$ and $-\frac{1}{2}m$, that render them divisible by m. For neither of them can have more than $\frac{m-1}{2}$ such values, by the foregoing proposition; and, since their product has $m-1$, it is obvious, that they have each the same number of values of x between the above limits, and that this number is $\frac{m-1}{2}$.

CHAP. VII.

On the Products and Transformations of certain Algebraical Formulæ.

PROP. I.

89. The product of the sum and difference of any two quantities is equal to the difference of their squares.

For,

$$(x+y)(x-y)=x^2-y^2. \qquad \text{Q. E. D.}$$

PROP. II.

90. The product of a sum of two squares, by double a square, is also the sum of two squares; or

$$(x^2+y^2) \times 2z^2 \mathrel{+\!\!\!\!=} x'^2+y'^2.$$

For,

$$(x^2+y^2) \times 2z^2 = (x+y)^2 . z^2 + (x-y)^2 . z^2,$$

which is evidently $\mathrel{+\!\!\!\!=} x'^2+y'^2$.

Cor. Hence if a number be the sum of two squares, its double is also the sum of two squares. Also if a number N be the sum of two squares, 2^nN is so likewise.

Thus, for example,

$$5=2^2+1^2; \quad 5 \times 2 = 10 = 3^2+1^2;$$

$$10 \times 2 = 20 = 4^2+2^2; \quad 20 \times 2 = 40 = 6^2+2^2 \text{ \&c.}$$

PROP. III.

91. The product arising from the sum of two squares by the sum of two squares, is also the sum of two squares; or

$$(x^2+y^2)(x'^2+y'^2)=x''^2+y''^2.$$

For,

$$(x^2+y^2)(x'^2+y'^2)=\begin{cases} (xx'+yy')^2+(xy'-x'y)^2, \\ \text{or } (xx'-yy')^2+(xy'+x'y)^2, \end{cases}$$

as will be evident from the development of these expressions; and, consequently,

$$(x^2+y^2)(x'^2+y'^2)=x''^2+y''^2. \qquad \text{Q. E. D.}$$

Cor. Hence the product may be divided into two squares two different ways. And if this product be again multiplied by another, that is the sum of two squares, the resulting product may be divided into two squares four different ways; and, generally, if a number N be the product of n factors, each of which is the sum of two squares, then will N be the sum of two squares, and may be resolved into two squares 2^n different ways.

For example, $\quad 5=2^2+1^2$

$\qquad\qquad\qquad\quad 13=3^2+2^2$

Then the product $65=8^2+1^2$, or 7^2+4^2.

Again, - - $\quad 17=4^2+1^2$

The product $\begin{cases} 1105=32^2+9^2=33^2+4^2=31^2+12^2 \\ \quad =24^2+23^2. \end{cases}$

And this resolution of the given product into square parts, is readily effected by the foregoing theorem; for

$$\begin{cases} (8^2+1)(4^2+1^2)=(4.8+1)^2+(8.1-4.1)^2= \\ \quad (4.8-1)^2+(8.1+4.1)^2, \text{ and} \end{cases}$$

$$\begin{cases} (7^2+4^2)(4^2+1)=(4.7+1.4)^2+(4.4-7.1)^2= \\ \quad (4.7-1.4)^2+(7.1+4.4)^2. \end{cases}$$

And in the same manner may any other product, arising from factors of this form, be resolved into its square parts.

PROP. IV.

92. The product of the sum of three squares, by the sum of two squares, is the sum of four squares; or

$$(x^2+y^2+z^2)(x'^2+y'^2) \doteq w''^2+x''^2+y''^2+z''^2.$$

For,

$$(x^2+y^2+z^2)(x'^2+y'^2)=$$
$$(xx'+yy')^2+(xy'-yx')^2+x'^2z^2+y'^2z^2,$$

as will appear immediately, from the development of these formulæ; and, consequently,

$$(x^2+y^2+z^2)(x'^2+y'^2) \doteq w''^2+x''^2+y''^2+z''^2.$$

Q. E. D.

For example, - $14=3^2+2^2+1^2$
$5=2^2+1$

Then the product $\left\{ \begin{array}{l} 70=(3.2+2.1)^2+(2.2-3.1)^2 \\ \quad +2^2+1^2=8^2+1^2+2^2+1^2; \end{array} \right.$

and a similar decomposition may be effected on any other similar product.

PROP. V.

93. The product arising from the sum of four squares, by the sum of two squares, is the sum of four squares; or

$$(w^2+x^2+y^2+z^2)(x'^2+y'^2) \doteq w'^2+x'^2+y'^2+z'^2.$$

For,

$$(w^2+x^2)(x'^2+y') \doteq w'^2+x'^2, \text{ and}$$
$$(y^2+z^2)(x'^2+y'^2) \doteq y'^2+z'^2,$$

by art. ~~89~~ 91; and, consequently,

$$(w^2+x^2+y^2+z^2)(x'^2+y'^2) \doteq w'^2+x'^2+y'^2+z'^2.$$

Q. E. D.

PROP. VI.

94. The product of the sum of four squares, by the sum of four squares, is also of the same form; or

$$\left\{ \begin{array}{l} (w^2+x^2+y^2+z^2)(w'^2+x'^2+y'^2+z'^2) \doteqdot \\ \quad w''^2+x''^2+y''^2+z''^2.) \end{array} \right.$$

For,

$$(w^2+x^2+y^2+z^2)(w'^2+x'^2+y'^2+z'^2) =$$
$$(ww'+xx'+yy'+zz')^2+(wx'-xw'+yz'-zy')^2+$$
$$(wy'-xz'-yw'+zx')^2+(wz'+xy'-yx'-zw')^2,$$

as will appear immediately from the development of the above formulæ; and, consequently, the product in question $\doteqdot (w''^2+x''^2+y''^2+z''^2)$.—Q. E. D.

Cor. 1. As in this product, there are only complete squares enter, we may change at pleasure the signs of the simple quantities; and, consequently, there will result several different formulæ equal to the same product, and each equal to the sum of four squares; and in so many different ways may any number that arises from the product of factors of the above form, be resolved into the sum of four squares.

Cor. 2. This proposition may be rendered more general by the following enunciation:

The product of the two formulæ,

$$(w^2-bx^2-cy^2+bcz^2)(w'^2-bx'^2-cy'^2+bcz'^2) \doteqdot$$
$$(w''^2-bx''^2-cy''^2+bcz''^2).$$

For,

$$(w^2-bx^2-cy^2+bcz^2)(w'^2-bx'^2-cy'^2+bcz'^2) =$$
$$\left\{ \begin{array}{l} (ww'+bxx' \pm cyy' \pm bczz')^2 - \\ b(wx'+w'x \pm cyz' \pm cy'z)^2 - \\ c(wy'-bxz' \pm yw' \mp bzx')^2 + \\ bc(xy'-wz' \pm zw' \mp yx')^2, \end{array} \right.$$

as will be evident from the development; and, consequently, the product in question is of the same form as each of its factors.

PROP. VII.

95. The product of the two formulæ $(x^2 - ay^2)$ and $(x'^2 - ay'^2)$, is of the same form as each of them; that is,

$$(x^2 - ay^2)(x'^2 - ay'^2) = x''^2 - ay''^2.$$

For,

$$(x^2 - ay^2)(x'^2 - ay'^2) = \begin{cases} (xx' + ayy')^2 - a(xy' + yx')^2, \\ \text{or } (xx' - ayy')^2 - a(xy' - xy')^2; \end{cases}$$

and, consequently,

$$(x^2 - ay^2)(x'^2 - ay'^2) = x''^2 - ay''^2.$$

Q. E. D.

Cor. The product of any number of factors, each of the form $(y^2 - ay^2)$, is always of the same form.

PROP. VIII.

96. The two formulæ

$$(x^2 + y^2 + z^2) \text{ and } (x^2 + y^2 + 2z^2),$$

are so related to each other, that the double of the one produces the other; that is,

$$(x^2 + y^2 + z^2) \times 2 = x'^2 + y'^2 + 2z'^2, \text{ and}$$
$$(x^2 + y^2 + 2z^2) \times 2 = x'^2 + y'^2 + z'^2.$$

For,

$$2(x^2 + y^2 + z^2) = 2x^2 + 2y^2 + 2z^2 =$$
$$(x + y)^2 + (x - y)^2 + 2z^2 = x'^2 + y'^2 + 2z'^2.$$

And

$$2(x^2 + y^2 + 2z^2) = 2x^2 + 2y^2 + 4z^2 =$$
$$(x + y)^2 + (x - y)^2 + 4z^2 = x'^2 + y'^2 + z'^2.$$

Q. E. D.

For example, $14 = 3^2 + 2^2 + 1^2$

Mult. by - 2

The product $\begin{cases} = 28 = (3+2)^2 + (3-2)^2 + 2 \,.\, 1^2 \\ = 5^2 + 1^2 + 2. \end{cases}$

And - - $15 = 3^2 + 2^2 + 2 \,.\, 1^2$

Mult. by - 2

The product $\begin{cases} = 30 = (3+2)^2 + (3-2)^2 + 2^2 \\ = 5^2 + 1^2 + 2^2. \end{cases}$

And the same of all other numbers of these forms.

PROP. IX.

97. The formula $x^2 - 2y^2$ may be always transformed to another of the form $2x'^2 - y'^2$, and this last may be converted into the former; that is,

$$\begin{cases} x^2 - 2y^2 = 2x'^2 - y'^2, \\ 2x^2 - y^2 = x'^2 - 2y'^2. \end{cases}$$

For,

$x^2 - 2y^2 = 2(x \pm y)^2 - (x \pm 2y)^2 = 2x'^2 - y'^2$, and

$2x^2 - y^2 = (x \pm 2y)^2 - 2(x \pm y)^2 = x'^2 - 2y'^2$;

as is evident from the development of these formulæ; and, consequently, a number that is of one of these forms is also of the other. — Q. E. D.

For example, $14 = 2 \,.\, 3^2 - 2^2 = 4^2 - 2 \,.\, 1^2$.

Also, - - $28 = 6^2 - 2 \,.\, 2^2 = 2 \,.\, 4^2 - 2^2$.

And the same of any other numbers of either of these forms.

PROP. X.

98. The formula $x^2 - 5y^2$ may be always transformed to another of the form $5x'^2 - y'^2$, and this last may be converted into the former; that is,

$$\begin{cases} x^2 - 5y^2 \mathrel{\underset{\cdot}{\overset{\cdot}{=}}} 5x'^2 - y'^2, \\ 5x^2 - y^2 \mathrel{\underset{\cdot}{\overset{\cdot}{=}}} x'^2 - 5y'^2. \end{cases}$$

For,

$x^2 - 5y^2 = 5(x \pm 2y)^2 - (2x \pm 5y)^2 \mathrel{\underset{\cdot}{\overset{\cdot}{=}}} 5x'^2 - y'^2$, and

$5x^2 - y^2 = (5x \pm 2y)^2 - 5(2x \pm y)^2 \mathrel{\underset{\cdot}{\overset{\cdot}{=}}} x'^2 - 5y'^2$;

and, consequently, any number that is of one of these forms is also of the other.

For example $29 = 7^2 - 5 . 2^2 = 5 . 11^2 - 24^2 = 5 . 3^2 - 4^2$

And - - $41 = 5 . 3^2 - 2^2 = 19^2 - 5 . 8^2 = 11^2 - 5 . 4^2$.

And a similar transformation may be made on any other number falling under either of the above forms.

PROP. XI.

99. If a be any number of the form $b^2 + 1$, then will the formula $x^2 - ay^2$ be resolvible into another of the form $ax^2 - y^2$; and, conversely, this last may be transformed into the former; that is,

$$\begin{cases} x^2 - (b^2+1)y^2 \mathrel{\underset{\cdot}{\overset{\cdot}{=}}} (b^2+1)x'^2 - y'^2, \text{ and} \\ (b^2+1)x^2 - y^2 \mathrel{\underset{\cdot}{\overset{\cdot}{=}}} x'^2 - (b^2+1)y'^2. \end{cases}$$

For,

$x^2 - (b^2+1)y^2 = (b^2+1)(x \pm by)^2 - \{bx \pm (b^2+1)y\}^2$,

and

$(b^2+1)x^2 - y^2 = \{(b^2+1)x \pm by\}^2 - (b^2+1)(bx+y)^2$,

the first of which transformed formulæ is evidently

$\mathrel{\underset{\cdot}{\overset{\cdot}{=}}} (b^2+1)x'^2 - y'^2$; also the latter

$\mathrel{\underset{\cdot}{\overset{\cdot}{=}}} x'^2 - (b^2+1)y'^2$; and, consequently,

$x^2 - ay^2 \mathrel{\underset{\cdot}{\overset{\cdot}{=}}} ax'^2 - y'^2$, and

$ax^2 - y^2 \mathrel{\underset{\cdot}{\overset{\cdot}{=}}} x'^2 - ay'^2$, when

$a \mathrel{\underset{\cdot}{\overset{\cdot}{=}}} b^2 + 1$.

Cor. These general formulæ furnish us with

many particular cases, which have the singular property of being convertible from one to the other; such are

$$\left\{\begin{array}{rcl} x^2 - 2y^2 & \pm & 2x'^2 - y'^2, \\ 2x^2 - y^2 & \pm & x'^2 - 2y'^2. \end{array}\right.$$

$$\left\{\begin{array}{rcl} x^2 - 5y^2 & \pm & 5x'^2 - y'^2, \\ 5x^2 - y^2 & \pm & x'^2 - 5y'^2. \end{array}\right.$$

$$\left\{\begin{array}{rcl} x^2 - 10y^2 & \pm & 10x'^2 - y'^2, \\ 10x^2 - y^2 & \pm & x'^2 - 10y'^2. \end{array}\right.$$

$$\left\{\begin{array}{rcl} x^2 - 17y^2 & \pm & 17x'^2 - y'^2, \\ 17x^2 - y^2 & \pm & x'^2 - 17y'^2. \end{array}\right.$$

&c. &c.

PROP. XII.

100. If m and n be the two roots of the quadratic equation $\phi^2 - a\phi + b = 0$, then will the product of the two formulæ $(x + my)$, and $(x + ny)$, be equal to $x^2 + axy + by^2$.

This is evident from the actual multiplication of the factors $(x + my)$ and $(x + ny)$.

For,

$$(x + my)(x + ny) = x^2 + (m + n)xy + mny^2;$$

and, since m and n are the roots of the equation $\phi^2 - a\phi + b = 0$, we have, from the nature of equations, $m + n = a$, and $mn = b$; and, consequently, the above product becomes

$$x^2 + axy + by^2.$$

Q. E. D.

Cor. Hence, conversely, every quantity of the form $x^2 + axy + by^2$ may be considered as the product arising from the multiplication of two factors, $(x + my)$ and $(x + ny)$, m and n being the roots of the quadratic equation

$$\phi^2 - a\phi + b = 0;$$

or, which is the same, m and n being such as to answer the conditions, $m + n = a$, and $mn = b$.

PROP. XIII.

101. The product arising from the multiplication of the two formulæ

$$x^2 + axy + by^2, \text{ and } x'^2 + ax'y' + by'^2,$$

is of the same form as each of them; that is,

$$(x^2 + axy + by^2)(x'^2 + ax'y' + by'^2) = (x''^2 + ax''y'' + by''^2).$$

For,

$$x^2 + axy + by^2 = (x + my)(x + ny), \text{ and}$$
$$x'^2 + ax'y' + by'^2 = (x' + my')(x' + ny');$$

and, therefore, the product in question is the same as the continued product of the four latter factors.

Now,

$$(x + my)(x' + my') = xx' + m(xy' + x'y) + m^2yy',$$

but since m is one of the roots of the equation

$$\phi^2 - a\phi + b = 0,$$

we have $m^2 - am + b = 0$, whence $m^2 = am - b$; and, substituting this value of m^2, in the above formula, it becomes

$$xx' - byy' + m(xy' + x'y + ayy').$$

And if, in order to simplify, we make

$$\text{X} = xx' - byy',$$
$$\text{Y} = xy' + yx' + ayy',$$

the product of the two factors,

$$(x + my)(x' + my') = \text{X} + m\text{Y};$$

and, in the same manner, we find

$$(x+ny)(x'+ny')=\text{X}+n\text{Y};$$

and, consequently, the whole product will be

$$(\text{X}+m\text{Y})(\text{X}+n\text{Y})=\text{X}^2+a\text{XY}+b\text{Y}^2;$$

that is, the product

$$\left\{\begin{array}{l}(x^2+axy+by^2)(x'^2+ax'y'+by'^2)=(x''^2+ax''y''+\\ \quad by''^2.\end{array}\right.$$

Cor. 1. Hence it follows, that the product of any number of factors of this form; as

$$\begin{array}{l} x^2+axy+by^2, \\ x'^2+ax'y'+by'^2, \\ x''^2+ax''y''+by''^2, \\ \&c. \qquad \&c. \end{array}$$

will always be of the same form as those factors.

Therefore, if we make $x=x'$, and $y=y'$, we shall have $\text{X}=x^2-by^2$, and $\text{Y}=2xy+ay^2$; and, consequently,

$$(x^2+axy+by^2)^2=\text{X}^2+a\text{XY}+b\text{Y}^2.$$

And, therefore, if it were required to make a square of the expression

$$\text{X}^2+a\text{XY}+b\text{Y}^2,$$

we shall only have to give to X and Y the preceding values, whence we readily obtain for the root of the square required the formula

$$x^2+axy+by^2,$$

where x and y may be any numbers at pleasure.

Ex. 1. Find the values of x and y in the equation

$$x^2+3xy+5y^2=z^2.$$

Here $a=3$ and $b=5$, therefore, the general values of x and y are

$$\begin{cases} x = t^2 - 5u^2, \\ y = 2tu + 3u^2, \end{cases}$$

where, for distinction sake, we write t and u, in the above formulæ, instead of x and y. Whence, by assuming successively,

$$t = 3,\ 4,\ 5,\ 6,\ \&c.,$$
$$u = 1,\ 1,\ 1,\ 1,\ \&c.,$$

we shall have the following corresponding values of x and y;

$$x = 4,\ 11,\ 20,\ 31,\ \&c.,$$
$$y = 9,\ 11,\ 13,\ 15,\ \&c.$$

Ex. 2. Find the values of x and y in the equation

$$x^2 - 7xy + 3y^2 = z^2.$$

Here, since $a = -7$ and $b=3$, the general values of x and y are

$$\begin{cases} x = t^2 - 3u^2, \\ y = 2tu - 7u^2. \end{cases}$$

And making now

$$t = 4,\ 5,\ 6,\ 7,\ 8,\ \&c.,$$
$$u = 1,\ 1,\ 1,\ 1,\ 1,\ \&c.,$$

we obtain

$$x = 13,\ 22,\ 33,\ 46,\ 61,\ \&c.,$$
$$y = 1,\ 3,\ 5,\ 7,\ 9,\ \&c.$$

Each of which corresponding values of x and y answer the required conditions of the equation; and it is manifest, that an infinite number of other values might be obtained, by changing those of t and u.

CHAP. VIII.

On the Quadratic Divisors of certain Algebraical Formulæ.

PROP. I.

102. If the indeterminate formula

$$py^2 + 2qyz + rz^2 = \phi,$$

the coefficients, p, q, and r, have not all three the same common divisor, and y and z be any numbers whatever prime to each other; and if $2q > p$, or $> r$, this formula may always be transformed to a similar one,

$$p'y'^2 + 2q'y'z' + r'z'^2 = \phi,$$

which shall be equal to the same quantity ϕ, and in which $2q'$ shall not exceed either p' or r'.

Let us suppose, first, $2q > p$; and in the case in which also $2q > r$, let p be the least of these two numbers p and r, abstracting from their signs. Now make $y = y' - mz$, m being an indeterminate coefficient; and substituting for this value of y in the given equation, we have

$$p(y' - mz)^2 + 2qz(y' - mz) + rz^2 = \phi, \text{ or}$$
$$py'^2 - 2(pm - q)y'z + (pm^2 - 2qm + r)z^2 = \phi.$$

And here we may always take the indeterminate quantity m, so that $\pm(pm - q) < p$ (art. 10). Calling, therefore, $\pm(pm - q) = q'$, and $(pm^2 - 2qm + r) = r'$, the transformed formula will be

$$py'^2 + 2q'y'z + r'z^2 = \phi,$$

in which $2q' < p$ (this sign not excluding equality), and in which $pr' - q'^2 = pr - q^2$, for

$$q'^2 = p^2m^2 - 2pqm + q^2,$$
$$pr' = p^2m^2 - 2pqm + rp,$$

therefore, by subtraction,

$$pr' - q'^2 = pr - q^2;$$

where these quantities will always have the same sign.

Now, since we have $2q > p$, and $2q' < p$, it follows that $q' < q$. We have, therefore, now, an equation,

$$py'^2 + 2q'y'z + r'z^2 = \phi,$$

in which the mean coefficient $2q'$, does not exceed the extreme coefficient p; and if at the same time it does not exceed the other extreme coefficient r', the formula is transformed as required. But if $2q'$, though $< p$, be $> r'$, we may proceed in a similar manner to obtain a new transformation, in which the mean coefficient (which we may represent by q'') shall be less than q', and so on again for others, in which the mean coefficient $2q'''$ is less than $2q''$. But the series of integers

$$q,\ q',\ q'',\ q''',\ \&c.,$$

cannot go on continually decreasing, without becoming finally less than the extreme coefficients; and, therefore, by continuing these transformations, we must necessarily at last arrive at that, which admits not of any farther reduction; and which will be consequently such, that the mean coefficient is less than either of the extremes, or at least not greater than the least of them; for with any

formula, in which this is not the case, a farther reduction may be made. Therefore, every formula,

$$py^2 + 2qyz + rz^2,$$

in which the mean coefficient $2q$ exceeds either, or both, of the extreme coefficients, may be transformed to another, in which the mean coefficient $2q$ shall be less than either of the extreme coefficients, or at least not greater than the least of them. — Q. E. D.

Cor. In the successive transformation of the formula,

$$\begin{aligned} &py^2 + 2q\,yz + rz^2, \text{ to} \\ &py'^2 + 2q'\,y'z + r'z^2, \text{ to} \\ &p'y'^2 + 2q''y'z' + r'z'^2, \text{ \&c.,} \end{aligned}$$

we have always

$$pr - q^2 = pr' - q'^2 = p'r' - q''^2, \text{ \&c.,}$$

each of these quantities having the same sign; for we have seen this equality take place in the transformation that we have effected, and it is evident, that the same would still have place in any farther reduction, the operations being all effected in the same manner.

The following example may be of some use in illustrating the foregoing proposition.

Let there be proposed the formula

$$35y^2 + 172yz + 210z^2 = \phi,$$

in which the mean coefficient 172 exceeds the first 35; and let it be required to transform this to another equal and similar one, in which the mean coefficient shall be less than either of the extremes.

First, put $y=y'-mz$, which value of y, being substituted in the given formula, gives

$$35y'^2-(70m-172)y'z+(35m^2-172m+210)z^2.$$

And now, in order that $70m-172<35$, take $m=2$, which reduces the above to

$$35y'^2+32y'z+6z^2=\phi,$$

in which the mean coefficient 32, though <35, is still >6; and, therefore, we must proceed to another similar reduction.

Let, then, $z=z'-my'$, and the second transformed formula will become

$$6z'^2-(12m-32)y'z'+(6m^2-32m+35)y'^2.$$

And here, taking $m=3$ in order that $12m-32<6$, we obtain

$$6z'^2-4z'y'-7y'^2=\phi,$$

and this last formula has the required conditions; because $4<6$ and <7.

And moreover, in these transformations, we have

$$pr-q^2=pr'-q'^2=p'r'-q''^2, \text{ or}$$
$$35\,.\,210-(66)^2=-46,$$
$$35\,.\quad 6-(16)^2=-46,$$
$$-6\,.\quad 7-(\ 2)^2=-46,$$

all equal, and with the same sign, as observed in the foregoing corollary.

PROP. II.

103. Every divisor of the formula t^2+au^2, in which t and u are prime to each other, and a any integer number whatever, positive or negative, is also a divisor of the formula q^2+a.

For let p represent any divisor of the formula t^2+au^2, so that

$$t^2+au^2=pp',$$

then it is evident, that p is prime to u, for otherwise t and u must have the same common measure, which is contrary to the hypothesis, because t is prime to u; we may, therefore, find two other numbers, q and y, such that $t=py+qu$, q being $+$ or $-$ as the case may require (art. 40): and if now we substitute this value of t, in the above expression, we obtain

$$p^2y^2+2pqyu+(q^2+a)u^2=pp';$$

or, dividing by p, we have

$$py^2+2qyu+\left(\frac{q^2+a}{p}\right)u^2=p';$$

and, consequently, since p' is an integer, $(q^2+a)u^2$ is divisible by p, but we have seen that u is prime to p, and, therefore, it must be the other factor, (q^2+a), that is divisible by p (cor. 5, art. 11); therefore, if p be a divisor of the formula t^2+au^2, t and u being prime to each other, it is also a divisor of the more simple formula q^2+a.—Q. E. D.

Cor. Hence, conversely, if p be not a divisor of the formula q^2+a, in which there is only one indeterminate quantity q, it cannot be a divisor of the more general formula t^2+au^2, in which there are two indeterminates prime to each other.

PROP. III.

104. Every divisor of the formula t^2+au^2, in which t and u are prime to each other, is of the form $py^2+2qyu+ru^2$, and in which formula

$pr - q^2 = a$, and $2q < p$ and $< r$, or at least not greater than either of them.

For, by the foregoing proposition, we have

$$py^2 + 2qyu + \left(\frac{q^2 + a}{p}\right)u^2 = p';$$

and, since $\frac{q^2 + a}{p}$ is an integer, make $\frac{q^2 + a}{p} = r$; then the above becomes

$$py^2 + 2qyu + ru^2 = p';$$

that is, the factor

$$p' = py^2 + 2qyu + ru^2;$$

but p' may equally represent any one of the factors or divisors of $t^2 + au^2$; and, consequently, every factor or divisor of the formula $t^2 + au^2$ is of the form

$$py^2 + 2qyu + ru^2.$$

And again, since $\frac{q^2 + a}{p} = r$; therefore, $pr - q^2 = a$.

And we have seen (art. 102) how every indeterminate formula,

$$py^2 + 2qyu + ru^2,$$

may be transformed to another similar and equal formula,

$$p'y^2 + 2q'yz + r'z^2,$$

in which the mean coefficient $2q' < p'$ and $< r'$ (the sign $<$ not excluding equality), and in which $pr - q^2$ is always equal to the same constant quantity a. And, consequently, every divisor of the formula $t^2 + au^2$ has its divisors contained in the formula

$$py^2 + 2qyz + rz^2,$$

and in which $2q$ does not exceed p or r, and also such that $pr - q^2 = a$. — Q. E. D.

Remark 1. Since $2q < p$, and $2q < r$, independently of the signs of these quantities, we have $4q^2 < pr$; and because $pr - q^2 = a$, it follows, that when a is negative pr is also negative; for otherwise $pr - q^2$ would not have the same sign as a, which we have seen always takes place in every transformation; and hence we readily draw the following corollaries, according as a is positive or negative.

Cor. 1. Every divisor of the formula $t^2 + au^2$, when a is positive, may be represented by the formula

$$py^2 + 2qyz + rz^2,$$

in which $pr - q^2 = a$; $2q < p$ and $< r$, and, consequently, $4q^2 < pr$; and, therefore, $pr - q^2 = a$, $> 3q^2$, or $q < \sqrt{\frac{a}{3}}$: this is evident, because when a is positive, p and r are both positive.

Cor. 2. Every divisor of the formula $t^2 - au^2$ may be represented by the formula

$$py^2 + 2qyz - rz^2;$$

in which $-pr - q^2 = -a$, or $pr + q^2 = a$, because, when a is negative, pr is necessarily so likewise; and, consequently, one of these quantities, p or r, is $+$ and the other $-$, and it is indifferent to which we give the sign $-$; and here, since $pr < 4q^2$, we have $a > 5q^2$, or $q < \sqrt{\frac{a}{5}}$.

Remark 2. We may have cases in which $p = r = 2q$; as, for example, when $p = 2$, $q = 1$, and $r = 2$; for then $2q$ does not exceed either

p or r, neither are p, q, and r, divisible by the same number, which condition is, therefore, strictly within the limits of the proposition; and hence it follows, that we must not consider the sign $<$ in the two expressions $q < \sqrt{\frac{a}{3}}$ and $q < \sqrt{\frac{a}{5}}$, to exclude equality.

PROP. IV.

105. Every divisor of the formula $t^2 + u^2$, t and u being prime to each other, is always of the same form $y^2 + z^2$. Or the sum of two squares, which are prime to each other, can only be divided by numbers that are also the sums of two squares.

For by cor. 1 of the foregoing proposition, every divisor of the formula $t^2 + au^2$ is included in the formula

$$py^2 + 2qyz + rz^2,$$

and in which $q < \sqrt{\frac{a}{3}}$, and $pr - q^2 = a$.

Now in the present case $a = 1$, therefore, $q < \sqrt{\frac{1}{3}}$, or $q = 0$, there being no integer $< \sqrt{\frac{1}{3}}$; and, since $pr - q^2 = 1$, we have $pr = 1$, and therefore $p = 1$, and $r = 1$; and, consequently, the above formula, which includes all the divisors of $t^2 + u^2$, becomes

$$y^2 + z^2;$$

that is, every divisor of the formula $t^2 + u^2$ is of the form $y^2 + z^2$, or every divisor of the sum of two squares, prime to each other, is also the sum of two squares. — Q. E. D.

Thus, for example, $65 = 8^2 + 1^2$ can only be divided by 13 and 5, both of which are the sums of two squares. Also $50 = 7^2 + 1$ have for divisors $2 = 1^2 + 1^2$, $5 = 2^2 + 1^2$, $10 = 3^2 + 1^2$, $25 = 4^2 + 3^2$. Again, $221 = 10^2 + 11^2$ is only divisible by 13 and 17, which are both the sums of two squares; and the same for all other numbers included in the formula $t^2 + u^2$, t and u being prime to each other.

PROP. V.

106. Every divisor of the formula $t^2 + 2u^2$, t and u being prime to each other, is of the same form $y^2 + 2z^2$. Or the divisors of the sum of a square, and double a square, are also the sum of a square, and double a square.

For every divisor of this formula $t^2 + au^2$ is contained in the formula

$$py^2 + 2qyz + rz^2;$$

in which $q < \sqrt{\frac{a}{3}}$, and $pr - q^2 = a$ (cor. 1, art. 104).

But in this case $a = 2$, therefore $q < \sqrt{\frac{2}{3}}$, or $q = 0$; also, since $pr - q^2 = 2$, we have $pr = 2$, whence $p = 2$, and $r = 1$, or $p = 1$, and $r = 2$; therefore, the above formula becomes

$$\begin{cases} 2y^2 + z^2, & \text{in the first case, and} \\ y^2 + 2z^2, & \text{in the second,} \end{cases}$$

which are two identical forms, by changing y into z, and z into y; consequently, every divisor of the formula $t^2 + 2u^2$ is also of the same form as itself.

Cor. 1. With regard to the divisor 2, it can only be of the form $y^2 + 2z^2$, when $y = 0$ and $z = 1$; so that, in this case, we have $0^2 + 2 . 1^2$.

As an example to this proposition, we may take $99 = 1 + 2 \cdot 7^2$, which can only be divided by

$$3 = 1^2 + 2 \cdot 1^2,$$
$$9 = 1^2 + 2 \cdot 2^2,$$
$$11 = 3^2 + 2 \cdot 1^2,$$
$$33 = 5^2 + 2 \cdot 2^2;$$

and it is the same with every number that is contained under the above form.

PROP. VI.

107. Every divisor of the formula $t^2 - 2u^2$, t and u being prime to each other, is of the same form $y^2 - 2u^2$. Or the difference of a square, and double a square, can only be divided by those numbers that are equal to the difference of a square and double a square.

For since every divisor of the formula $t^2 - au^2$ is contained in the formula

$$py^2 + 2qyz - rz^2,$$

in which $pr + q^2 = a$, and also $q < \sqrt{\frac{a}{5}}$, or $< \sqrt{\frac{2}{5}}$ (cor. 2, art. 104), it follows that $q = 0$, whence also $pr = 2$; and, therefore, $p = 2$ and $r = 1$, or $p = 1$ and $r = 2$; and, consequently, the above formula becomes either

$$2y^2 - z^2, \text{ or } y^2 - 2z^2,$$

which two forms are precisely the same, because

$$2y^2 - z^2 = (2y \pm z)^2 - 2(y \pm z)^2;$$

therefore, every divisor of the formula $t^2 - 2u^2$ is also of the same form. Or the difference of a square, and double a square, can only be divided

by numbers that are also the difference of a square and double a square.

For example, $98 = 10^2 - 2 \cdot 1^2$ can only be divided by

$$2 = 2^2 - 2 \cdot 1^2,$$
$$7 = 3^2 - 2 \cdot 1^2,$$
$$14 = 4^2 - 2 \cdot 1^2,$$
$$49 = 9^2 - 2 \cdot 4^2;$$

and the same of all other numbers in this formula.

PROP. VII.

108. Every odd divisor of the formula $t^2 + 3u^2$ is also of the same form $y^2 + 3z^2$.

For since all its divisors are contained in the formula

$$py^2 + 2qyz + rz^2,$$

in which $pr - q^2 = a$, or $pr - q^2 = 3$; and also $q =$ or $< \sqrt{\frac{3}{3}}$ (*Remark* 2, art. 104), so that $q = 1$, or $q = 0$; therefore, in the first case, since $2q$ is not greater than p or r, and $pr - q^2 = 3$, we must have $p = 2$, and $r = 2$, which renders the above formula

$$2y^2 + 2qyz + 2z^2;$$

but as this is evidently an even divisor, it does not belong to the case at present under consideration, which only relates to the odd divisors of the given formula.

In our case, therefore, $q = 0$; and, consequently, $pr - q^2 = 3$, or $pr = 3$; therefore, $p = 3$ and $r = 1$, or $p = 1$ and $r = 3$; whence the above formula is reduced to

$$3y^2 + z^2, \text{ or } y^2 + 3z^2,$$

two expressions which are identical as to their form; and, therefore, every odd divisor of the formula $t^2 + 3u^2$ is also of the form $y^2 + 3z^2$.

Remark. With regard to the divisor 3, it is obvious that we must have $y^2 = 0$, and $z = 1$; or $3 = 0^2 + 3 \cdot 1^2$; but for all other divisors this exception has not place.

For example, $5^2 + 3 \cdot 6^2 = 133 = 7 \cdot 19$; and $7 = 2^2 + 3 \cdot 1^2$, also $19 = 4^2 + 3 \cdot 1^2$, both of the same form.

PROP. VIII.

109. Every odd divisor of the formula $t^2 - 5u^2$ is also of the same form $y^2 - 5z^2$.

For all its divisors are contained in the formula

$$py^2 + 2qyz - rz^2,$$

in which $-pr - q^2 = -a$, or $pr + q^2 = 5$, and $q =$ or $< \sqrt{\frac{5}{5}}$; and, consequently, $q = 1$ or 0; but the first case gives only even divisors, the same as in the foregoing proposition; and the latter case of $q = 0$ reduces the above formula to

$$5y^2 - z^2, \text{ or } y^2 - 5z^2,$$

which are identical forms; because

$$5y^2 - z^2 = (5y \pm 2z)^2 - 5(2y \pm z)^2;$$

and, consequently, every odd divisor of the formula $t^2 - 5u^2$ is itself of the same form.

As an example in this case, we may assume $95 = 10^2 - 5 \cdot 1^2$, which is only divisible by 5 and 19. Now $5 = 5^2 - 5 \cdot 2^2$, and $19 = 7^2 - 5 \cdot 2^2$; and the same of all other numbers in the above form.

Scholium. From the foregoing propositions it

appears, that all numbers which are comprised in the following formulæ, *viz.*

$$t^2+u^2,\ t^2+2u^2,\ t^2-2u^2,\ t^2+3u^2, \text{ and } t^2-5u^2,$$

t and u being prime to each other, can only have divisors that are of the same form. It is only necessary to except those divisors of the two latter forms,

$$t^2+3u^2, \text{ and } t^2-5u^2,$$

that are double of an odd number; the reason for which exception is explained in arts. 108 and 109.

It frequently happens, that a number falls under two or more of the above forms, in which case its divisors are also of the same double or treble forms. And in some cases we have numbers that belong to each of the forms above given. Thus

$$241=15^2+4^2=13^2+2.6^2=21^2-2.10^2=7^2+3.8^2= 31^2-5.12^2.$$

CHAP. IX.

On the Quadratic Forms of Prime Numbers, with Rules for determining them in certain Cases.

Lemma.

110. Since all square numbers are of one of the forms $4n$, or $8n+1$, we establish at once the three following *theorems*:

1. Every odd number represented by the formula

$$y^2+z^2 \doteq 4n+1.$$

2. Every odd number represented by the formula

$$y^2+2z^2 \doteq 8n+1, \text{ or } 8n+3.$$

3. Every odd number represented by the formula

$$y^2-2z^2 \doteq 8n+1, \text{ or } 8n+7.$$

And from these three arise, by way of exclusion, three others; *viz.*

4. No number of the form $4n-1$ can be represented by the formula y^2+z^2.

5. No number of the form $8n+5$, or $8n+7$, can be represented by the formula y^2+2z^2.

6. No number of the form $8n+3$, or $8n+5$, can be represented by the formula y^2-2z^2.

PROP. I.

111. Every prime number of the form $4n+1$ is the sum of two squares, or is contained in the formula y^2+z^2.

For let m represent a prime number of this form, or $m = 4n + 1$; then (art. 87)

$$(x^{m-1} - 1) = \text{M}(m), \text{ or } (x^{4n} - 1) = \text{M}(m).$$

But $x^{4n} - 1 = (x^{2n} + 1)(x^{2n} - 1)$, and each of these factors has $2n$ values of x contained between the limits $+\frac{1}{2}m$ and $-\frac{1}{2}m$, that render them divisible by m (cor. 1, art. 88), whence the factor $x^{2n} + 1$ is divisible by m; but $x^{2n} + 1$ is the sum of two squares, and therefore its divisor m is also the sum of two squares; because every divisor of the formula $t^2 + u^2$ is itself of the same form (art. 105).—Q. E. D.

Cor. 1. As the form $4n + 1$ includes the two, $8n + 1$ and $8n + 5$; therefore, every prime number contained in these two latter forms is also the sum of two squares.

Thus, 5, 13, 17, 29, 37, and 41, are prime numbers of the form $4n + 1$, and each of these is the sum of two squares; for $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1$, $29 = 5^2 + 2^2$, $37 = 6^2 + 1^2$, and $41 = 5^2 + 4^2$; and so on for all other prime numbers of this form.

Cor. 2. We have seen (art. 91) that every number, which is produced from the multiplication of factors that are the sums of two squares, is itself of the same form, and may be resolved into two squares different ways, according to the number of its factors; and hence we may find a number, that is resolvible into two squares as many ways as we please, by multiplying together different prime numbers of the form $4n + 1$.

PROP. II.

112. Every prime number $8n + 1$ is of the three forms $y^2 + z^2$, $y^2 + 2z^2$, and $y^2 - 2z^2$.

For let m be a prime number of the form $8n+1$, or $m=8n+1$; then, as this form is included in that of $4n+1$, we know, from the foregoing proposition, that $m=y^2+z^2$; and it therefore only remains to demonstrate the two latter cases.

Now since $(x^{m-1}-1)=\text{M}(m)$, or $(x^{8n}-1)=\text{M}(m)$ (art. 87), we may put this under the form

$$(x^{4n}+1)(x^{4n}-1);$$

and each of these factors will have $4n$ values of $x<\frac{1}{2}m$, that render them divisible by m (cor. 1, art. 88), so that there are so many different values of x, that render the binomial $x^{4n}+1$ divisible by m; but this may be put under the form $(x^{2n}-1)^2+2x^{2n}$, and m being a divisor of this formula, it is itself of the same form y^2+2z^2 (art. 106).

We may also put the same quantity $x^{4n}+1$, under the form $(x^{2n}+1)^2-2x^{2n}$; and m being also a divisor of this formula, is itself of the same form y^2-2z^2 (art. 107).

Hence, every prime number of the form $8n+1$ is of the three forms y^2+z^2, y^2+2z^2, and y^2-2z^2.

Q. E. D.

Thus $41=5^2+4^2=3^2+2\,.\,4^2=7^2-2\,.\,2^2$,

And $73=8^2+3^2=1^2+2\,.\,6^2=9^2-2\,.\,2^2$.

PROP. III.

113. Every prime number $8n+3$ is of the form

$$y^2+2z^2.$$

For let m be a prime number of this form, or $m=8n+1$; then we have (by art. 87)

$$(x^{m-1}-1)=\text{M}(m), \text{ or } (x^{8n+2}-1)=\text{M}(m);$$

and there are $8n+2$ values of x contained in the

series 1, 2, 3, 4, &c., $8n+2$, that render this formula divisible by m (cor. 1, art. 87); and, consequently, $(2^{8n+2}-1) = \text{M}(m)$.

But $2^{8n+2}-1 = (2^{4n+1}+1)(2^{4n+1}-1)$, and, therefore, one of these factors is divisible by m; and it cannot be the latter, because this may be written $2 \,.\, 2^{4n}-1$, which is of the form $2t^2-u^2$, or t^2-2u^2; and, therefore, if m was a divisor of this, it would be itself of the same form (art. 107), or $m \doteq y^2-2z^2$; but this formula cannot represent any number of the form $8n+3$ (art. 110), whence, since m cannot be a divisor of this factor, it must therefore be a divisor of the other factor $2^{4n+1}+1$. But

$$2^{4n+1}+1 = 2 \,.\, 2^{4n}+1 \doteq 2t^2+u^2;$$

and, consequently, its divisor m is of the same form (art. 106); that is, $m \doteq y^2+2z^2$. — Q. E. D.

For example, 11, 19, and 43, are prime numbers of the above form; and $11 = 3^2+2 \,.\, 1^2$, $19 = 1^2+2 \,.\, 3^2$, and $43 = 5^2+2 \,.\, 3^2$; and the same of others.

PROP. IV.

114. Every prime number $8n+7$ is of the form

$$y^2-2z^2.$$

For let m be a prime number of this form, or $m = 8n+7$; then we have (by art. 87)

$$(x^{m-1}-1) = \text{M}(m), \text{ or } (x^{8n+6}-1) = \text{M}(m);$$

and there are $8n+6$ values of x, contained in the series 1, 2, 3, 4, &c., $8n+6$, that render this formula divisible by m (cor. 1, art. 87); and, consequently,

$$(2^{8n+6}-1) = \text{M}(m).$$

But $2^{8n+6}-1 = (2^{4n+3}+1)(2^{4n+3}-1)$, and there-

fore one of these factors is divisible by m; and, consequently, m will also be a divisor of one of them when doubled; that is, it is a divisor of one of the two quantities

$$2(2^{4n+3}+1), \text{ or } 2(2^{4n+3}-1),$$

which two expressions thus become

$$2^{4n'}+2\cdot 1^2, \text{ and } 2^{4n'}-2\cdot 1^2,$$

and m is necessarily a divisor of one of them. But it cannot be a divisor of the first, because this being of the form t^2+2u^2, if m was a divisor of it, we should have $m \doteq y^2+2z^2$ (art. 106); but $m \doteq 8n+7$, and no odd number of the form y^2+2z^2 is of the form $8n+7$ (art. 110): since, therefore, m is not a divisor of this factor, it must necessarily be a divisor of the other factor $2^{4n'}-2\cdot 1^2$, which is of the form t^2-2u^2; and, consequently, its divisor m is also of the same form (art. 107); that is, $m \doteq y^2-2z^2$.

Q. E. D.

For example, $31=7^2-2\cdot 3^2$, and $47=7^2-2\cdot 1^2$; and the same of all other prime numbers in this form.

Scholium. From the last four propositions, we may draw the following *theorems*:

1. All prime numbers of the forms $8n+1$, and $8n+5$, are, exclusively of all others, contained in the formula y^2+z^2.

2. All prime numbers of the form $8n+1$, and $8n+3$, are, exclusively of all others, contained in the formula y^2+2z^2.

3. All prime numbers of the form $8n+1$, and $8n+7$, are, exclusively of all others, contained in the formula y^2-2z^2.

4. All prime numbers of the form $8n+1$ are, at the same time, of the three forms

$$y^2+z^2,\ y^2+2z^2,\ \text{and}\ y^2-2z^2.$$

PROP. V.

115. To ascertain whether a given number of the form $4n+1$ be a prime number.

Since every prime number p of the form $4n+1$ is the sum of two squares, or $p=x^2+y^2$, it is obvious, that in order to determine whether a given number of this form be a prime, we have only to ascertain whether it can be resolved into two squares; and, if it can, in how many ways this resolution may be effected; then, if it happen that the given number may be decomposed into two squares, in one way only, the number is a prime, but otherwise it is composite; and the object of the present proposition is to teach the easiest method of performing this decomposition. Now, because $p=x^2+y^2$, and since these squares cannot be equal, it necessarily follows, that one of them is greater and the other less than $\frac{1}{2}p$; if, therefore, every square $>\frac{1}{2}p$ and $<p$ be subtracted from p, there ought to be found amongst the remainders one square number only, if the given number be a prime; and if there be no square remainder, or more than one, it will be a composite number.

Thus the number of operations in subtraction will not much exceed those in division, by the common rule; and the following observations will considerably abridge them, and, with the assistance of a small table of squares, render the method nearly as simple as can be expected, at least it is much

easier than any rule I have ever seen: which abridgment depends upon the following considerations.

Every prime number > 5 is of one of the forms $10n+1$, 3, 7, or 9; or, which is the same, it is terminated by one of those digits. Again, all squares are of one of the forms $10n$, $10n+1$, 4, 5, 6, or 9; or they are terminated in one of the digits, 0, 1, 4, 5, 6, or 9; and therefore no number terminating in 2, 3, 7, or 8, can be a square number; therefore,

1. When the last digit of the proposed number is 1, we may omit all squares terminating in 4, or 9, because these will give remainders terminating in 7, or 2, and, therefore, such remainders cannot be squares.

2. When the last digit of the given number is 3, we may omit all squares that terminate in 0, 1, 5, or 6; because these would give remainders terminating in 3, 2, 8, and 7; which, therefore, cannot be squares.

3. If the last digit be 7, we may omit all squares terminating in 0, 4, 5, or 9, for the same reason as above.

4. If the last digit be 9, we may omit all squares terminating in 1 or 6.

By these remarks the number of operations in subtraction will be reduced, generally, about one half, and will be considerably less than the number of operations in division by the common rule.

Ex. 1. Let it be proposed to ascertain whether the number 10133 be a prime.

Since this number terminates in 3, the only

squares between 5066 and 10133, that do not terminate in 0, 1, 5, or 6, are the following; *viz.*

Given N°.		*Squares.*		*Remainders.*
10133	−	5329	=	4804
10133	−	5929	=	4204
10133	−	6084	=	4049
10133	−	6724	=	3409
10133	−	6889	=	3244
10133	−	7569	=	2564
10133	−	7744	=	2389
10133	−	8464	=	1669
10133	−	8649	=	1484
10133	−	9409	=	724
10133	−	9604	=	529

Here the last remainder is $529 = 23^2$, and it is the only square; therefore, the given number 10133 is a prime.

Thus eleven operations in subtraction are made to answer the purpose of twenty-four divisions, and even this supposes all prime numbers under 100 to be known; for otherwise the number of divisions would be much more considerable.

Ex. 2. Is 7129 a prime number?

Ex. 3. Find whether 47933 be a prime number.

Ex. 4. Find whether 47881 be a prime number.

PROP. VI.

116. To ascertain whether a given number of the form $8n+3$ be a prime number.

Every prime number p of the form $8n+3$ is also of the form x^2+2y^2, or $p = x^2+2y^2$; and here x and y must be both odd squares, for otherwise

x^2+2y^2 could not have the form $8n+3$; also y^2 is necessarily less than $\frac{1}{2}p$; we must, therefore, subtract from p the double of every odd square $< \frac{1}{2}p$, and if amongst the remainders there be found one square, and no more, the given number is a prime; but otherwise it is not.

These operations may be considerably abridged from the following considerations:

We have seen, that all prime numbers terminate in one of the digits 1, 3, 7, or 9; and the doubles of square numbers terminate in one of the digits 0, 2, or 8; therefore,

1. If the given number terminate in 1, we may omit all those squares, the doubles of which terminate in 8; because these would have remainders terminating in 3, which cannot be squares.

2. If the last digit of the given number be 3 or 7, we may omit all squares the doubles of which terminate in 0, because the remainders of these will terminate in 3 or 7, and, therefore, are not squares.

3. If the last digit of the given number be 9, we may omit all squares, the doubles of which terminate in 2; because these will leave remainders terminating in 7, which cannot be squares.

4. It may be farther remarked, that every odd square has the last digit but one even, and, therefore, in general, all those double squares may be omitted, that leave an odd digit in the last place but one of the remainder.

Ex. Let it be proposed to ascertain whether the number 11051, which is of the form $8n+3$, be a prime number.

Here, the last digit being 1, we may omit all those squares terminating in 9, because the doubles of these terminate in 8, and, therefore, the remainders in 3. Hence the operation,

Given N°.		*Double Squares.*		*Remainders.*
11051	−	10082	=	969
11051	−	9522	=	1529
11051	−	8450	=	$2601 = 51^2$
11051	−	7442	=	3609
11051	−	6962	=	4089
11051	−	6050	=	5001
11051	−	5202	=	5849
11051	−	4802	=	6249
11051	−	4050	=	7001
11051	−	3362	=	7689
11051	−	3042	=	8009
11051	−	2450	=	8601
11051	−	1922	=	9129
11051	−	1682	=	9369
11051	−	1250	=	$9801 = 99^2$

Having thus found two square remainders, we may conclude with certainty, that the given number is not a prime, and discontinue the operation.

Remark. Our first rule extends to all numbers of the form $4n+1$, which includes the two forms $8n+1$ and $8n+5$, and the above applies to all numbers of the form $8n+3$; but those that fall under the form $8n+7$ are still excluded, nor can they be submitted to a similar test; for these numbers being of the form x^2-2y^2 (art. 114), there are no limits to the values of x and y, nor to the num-

ber of ways in which a given number may be resolved into this form; for

$$(x^2 - 2y^2) \times (x'^2 - 2y'^2)$$

may be resolved two ways into the same form (art. 95): and, since we may find $x'^2 - 2y'^2 = 1$, by taking $x = 3$ and $y = 2$, it follows, that this product is still $= x^2 - 2y^2$, that is, a number of the form $x^2 - 2y^2$ may be resolved into this form in as many ways as we please, whether it be a prime number or not, which is not the case with the two forms $x^2 + y^2$ and $x^2 + 2y^2$.

PROP. VII.

117. If a be any prime number, and the series of squares

$$1^2,\ 2^2,\ 3^2,\ 4^2,\ \&c.,\ \left(\frac{a-1}{2}\right)^2$$

be divided by a, they will each leave a different positive remainder.

This is in fact only a particular case of the general proposition demonstrated (art. 51); for, by making $\phi = 1$, the series of squares,

$$\phi^2,\ 2^2\phi^2,\ 3^2\phi^2,\ 4^2\phi^2,\ \&c.,\ \left(\frac{a-1}{2}\right)\phi^2,$$

becomes

$$1^2,\ 2^2,\ 3^2,\ 4^2\ \&c.,\ \left(\frac{a-1}{2}\right)^2,$$

each of which, when divided by a, will leave a different remainder, as is demonstrated in that article.

Cor. 1. And the same is evidently true of the

negative remainders, which arise from taking the quotients in excess (cor. 1, art. 51).

Cor. 2. Hence, also, we may see in what cases the positive and negative remainders are equal to each other; for then it is evident, that a will be a divisor of the sum of two squares, and we shall have

$$\frac{r^2+s^2}{a}=e, \text{ an integer number.}$$

Therefore, when a is not a divisor of the sum of two of these squares, the positive and the negative remainders are all different from each other, and include every number from 1 to $a-1$.

Cor. 3. When a is not a divisor of the sum of two squares, that is, when all the positive and negative remainders are different from each other, then some of each of those remainders are *greater*, and some *less*, than $\frac{1}{2}a$. For all the consecutive squares under a will be found amongst the positive remainders, and some of these squares must necessarily be *greater*, and some *less*, than $\frac{1}{2}a$; and, since the positive and negative remainders together include all numbers from 1 to $a-1$, the same is manifestly true for the negative remainders.

PROP. VIII.

118. If a be a prime number, it is always possible to find four squares, w^2, x^2, y^2, z^2 (the roots of each of which shall be less than $\frac{1}{2}a$), such that their sum may be divisible by a, or the equation

$$w^2+x^2+y^2+z^2=aa'$$

is always possible, a being any prime number whatever.

First, when the prime number a is a divisor of the sum of two squares, the proposition is evident; and it will, therefore, only be necessary to consider the case in which a is not a divisor of the sum of two squares, and, consequently, when all the remainders of the consecutive squares are different from each other (cor. 2, art. 117).

Now, in this case, we shall find some of the positive remainders *greater*, and some *less*, than $\frac{1}{2}a$; and the same of the negative remainders (cor. 3, art. 117). It is, therefore, always possible to find two squares, such that each being divided by a, the positive remainder of the one shall exceed the negative remainder of the other, by unity: and also two other squares in the same series, such that each being divided as before, the negative remainder of the one shall exceed the positive remainder of the other, by unity; that is, the equations $w^2 + x^2 - 1 = ma$, and $y^2 + z^2 + 1 = na$, are always possible, which may be demonstrated as follows:

Let p be the least negative remainder, then $p + 1$ must be found amongst either the positive or negative remainders; if it be found amongst the positive remainders, we have at once a positive remainder, that exceeds a negative remainder, by unity; and if it be not found amongst the positive, then $p + 1$ is still negative: and $p + 2$ must be either a positive or negative remainder; if it be positive, we have a positive remainder exceeding a negative one, by unity, but if not, $p + 2$ is still negative, and $p + 3$ must be either positive or negative; and proceeding thus, we must necessarily (as some of each of these

remainders are greater, and some less, than $\frac{1}{2}a$) arrive at that negative remainder p', such that $p'+1$ shall be a positive one; and, consequently, the equation $w^2+x^2-1=ma$ is always possible: and, in the same manner, the possibility of the equation $y^2+z^2+1=na$ may be demonstrated.

Having thus proved the possibility of the equations $w^2+x^2-1=ma$, and $y^2+z^2+1=na$, we have

$$\frac{w^2+x^2+y^2+z^2}{a}=m+n, \text{ an integer; or}$$

$$w^2+x^2+y^2+z^2=aa'$$

always possible. — Q. E. D.

Cor. It is obvious, from the foregoing demonstration, that these roots w, x, y, z, are less than $\frac{1}{2}a$; because we have only considered the squares contained in the series

$$1^2,\ 2^2,\ 3^2,\ 4^2,\ \&c.,\ \left(\frac{a-1}{2}\right)^2.$$

But, independently of this limitation, it may readily be shown, that if a be a divisor of the sum of any four squares, $w^2+x^2+y^2+z^2$, each of which is prime to a, that it is also a divisor of the sum of the four squares

$$(w-\alpha a)^2+(x-\beta a)^2+(y-\gamma a)^2+(z-\delta a)^2,$$

in which it is manifest, that α, β, γ, δ, may be always so assumed, that $\pm(w-\alpha a)\pm(x-\beta a)$, &c., shall be less than $\frac{1}{2}a$; whenever, therefore, it is demonstrated, that any number a is a divisor of the sum of four squares, we may always consider each of their roots as less than $\frac{1}{2}a$.

PROP. IX.

119. Every prime number a is the sum of two, three, or four squares.

For, by the foregoing proposition, the equation

$$w^2 + x^2 + y^2 + z^2 = aa'$$

is always possible, each of the roots of these squares being less than $\frac{1}{2}a$; and, consequently, each of the squares less than $\frac{1}{4}a^2$, whence we have $aa' < a^2$, or $a' < a$. Now, if $a' = 1$, it is evident that

$$w^2 + x^2 + y^2 + z^2 = a,$$

and the proposition will be demonstrated.

But if $a' > 1$, then, because a' is a divisor of the formula

$$w^2 + x^2 + y^2 + z^2,$$

it is also a divisor of the formula

$$(w - \alpha a')^2 + (x - \beta a')^2 + (y - \gamma a')^2 + (z - \delta a')^2,$$

where each of the roots is less than $\frac{1}{2}a'$ (cor., art. 118); assuming, therefore,

$$(w - \alpha a')^2 + (x - \beta a')^2 + (y - \gamma a')^2 + (z - \delta a')^2 = a''a',$$

we shall have, for the same reason as above,

$$a''a' < a'^2, \text{ or } a'' < a'.$$

Now, by means of the formula (art. 94), if we multiply together the values of aa', and $a''a'$, we shall find a product that is the sum of four squares, and of which each is divisible by a'^2; and having performed this division, we obtain

$$a''a = (a - \alpha w - \beta x - \gamma y - \delta z)^2 + (\alpha x - \beta w + \gamma z - \delta y)^2$$
$$+ (\alpha y - \gamma w + \delta x - \beta z)^2 + (\alpha z - \delta w + \beta y - \gamma x)^2;$$

or, for the sake of abridging this expression,

$$w'^2 + x'^2 + y'^2 + z'^2 = a''a\,;$$

and here we have $a'' < a'$. If now $a'' = 1$, the above becomes

$$w'^2 + x'^2 + y'^2 + z'^2 = a,$$

and the proposition will be demonstrated; but if a'', though $< a'$, be > 1, we may proceed, in the same manner, to find a new product,

$$w''^2 + x''^2 + y''^2 + z''^2 = a'''a.$$

and in which $a''' < a''$; and by continuing thus the decreasing series of integers a, a', a'', a''', a'''', &c., we must necessarily, finally, arrive at a term $a^{(m)}$ equal to unity, and then we shall have a equal to the sum of four squares. — Q. E. D.

PROP. X.

120. Every integral number whatever is either a square, or the sum of two, three, or four squares.

This follows immediately from the foregoing proposition, and the formula (art. 94); for every number is either a prime, or produced by the multiplication of prime factors; and since every prime number is of the form

$$(w^2 + x^2 + y^2 + z^2),$$

and the product of two or more such formulæ being still of the same form (art. 94), it necessarily follows, that every integral number whatever is of the form

$$(w^2 + x^2 + y^2 + z^2).$$

But it is to be observed, that no limitation in the course of the demonstration of the foregoing pro-

position was made, that could prevent any one or more of these squares from becoming zero; therefore, every integral number whatever is either a square, or the sum of two, three, or four squares.

Q. E. D.

Cor. All that has been proved in the foregoing proposition for integral numbers, is equally true of fractions; for every fraction may be expressed by an equivalent one having a square denominator; therefore, every fraction is of the form

$$\frac{w^2+x^2+y^2+z^2}{m^2}=\frac{w^2}{m^2}+\frac{x^2}{m^2}+\frac{y^2}{m^2}+\frac{z^2}{m^2};$$

this curious property, therefore, extends to every rational number whatever.

Scholium. The theorem that we have demonstrated, in the two foregoing propositions, forms a part of a general property of polygonal numbers, discovered by Fermat; which is this, "Every number is either a triangular number, or the sum of two or three triangular numbers. A square, or the sum of two, three, or four squares. A pentagonal, or the sum of two, three, four, or five pentagonals. And so on for hexagonals, &c. Or the same may be more generally expressed thus: If m represent the denomination of any order of polygonals, then is every number N the sum of m polygonals of that order; it being understood that any of these polygonals may become zero.

Let, therefore, N be any given number, and x, y, z, indeterminate quantities; then the different parts of the general theorem may be detailed in the following order:

1st, $N = \frac{x^2+x}{2} + \frac{y^2+y}{2} + \frac{z^2+z^2}{2}$;

2d, $N = w^2 + x^2 + y^2 + z^2$;

3d, $N = \frac{3u^2-u}{2} + \frac{3w^2-w}{2} + \frac{3x^2-x}{2} + \frac{3y^2-y}{2} + \frac{3z^2-z}{2}$;

4th, &c. &c. &c. &c.

The second form which relates to the squares has been demonstrated in the foregoing proposition, and Legendre has also demonstrated the first case, for triangular numbers; but all the other cases, past the second, still remain without demonstration, notwithstanding the researches and investigations of many of the ablest mathematicians of the present time, and of others now no more: amongst the former we may mention Lagrange, Legendre, and Gauss; and of the latter, Euler, Waring, and Fermat himself; the latter of whom, however, as appears from one of his notes on Diophantus, was in possession of the demonstration, although it was never published, which circumstance renders the theorem still more interesting to mathematicians, and the demonstration of it the more desirable.

We have demonstrated the second case, but this carries us no farther, whereas, if we had demonstrated the first, the second would flow from it as a corollary; and it may not be uninteresting to show in what manner these different parts of the same theorem are connected with each other.

First, let us suppose the possibility of the equation

$$N = \frac{x^2+x}{2} + \frac{y^2+y^2}{2} + \frac{z^2+z}{2}$$

to have been demonstrated, from which may be drawn this,

$$8N+3=(2x+1)^2+(2y+1)^2+(2z+1)^2, \text{ or}$$
$$8N+3=x'^2+y'^2+z'^2, \text{ or}$$
$$8N+4=x'^2+y'^2+z'^2+1;$$

and since these four squares are all odd, the numbers $x'+y'$, $x'-y'$, $z'+1$, and $z'-1$, are all even; and hence we have, in integers,

$$4N+2=$$
$$\left(\frac{x'+y'}{2}\right)^2+\left(\frac{x'-y'}{2}\right)^2+\left(\frac{z'+1}{2}\right)^2+\left(\frac{z'-1}{2}\right)^2,$$

or, for the sake of abridging,

$$4N+2=w''^2+x''^2+y''^2+z''^2;$$

of which squares two are even and two odd, for otherwise their sum could not have the form $4N+2$; we may, therefore, write

$$4N+2=4r^2+4s^2+(2t+1)^2+(2v+1)^2;$$

from which we deduce

$$2N+1=(r+s)^2+(r-s)^2+(t+v+1)^2+(t-v)^2;$$

that is, every odd number is the sum of four squares, and the double of a number that is the sum of four squares is itself the sum of four squares, for

$$\left\{\begin{array}{l} 2(m^2+n^2+p^2+q^2)= \\ (m+n)^2+(m-n)^2+(p+q)^2+(p-q)^2; \end{array}\right.$$

and, therefore, every number is the sum of four squares.

If, therefore, the case which relates to triangular numbers was demonstrated, that which relates to squares would be readily deduced from it; but the

converse has not place; that is, we cannot deduce the first case from the second.

The third case gives

$$\text{N} = \frac{3u^2 - u}{2} + \frac{3w^2 - w}{2} + \frac{3x^2 - x}{2} + \frac{3y^2 - y}{2} + \frac{3z^2 - z}{2}, \text{ or}$$

$$24\text{N} + 5 =$$
$$(6u - 1)^2 + (6w - 1)^2 + (6x - 1)^2 + (6y - 1)^2 + (6z - 1)^2.$$

So that the enunciation of this particular part returns to this,

Every number of the form $24\text{N} + 5$ *is the sum of five squares, of which each of the roots is of the form* $6n - 1$.

The fourth case returns to this,

Every number of the form $8\text{N} + 6$ *may be decomposed into six squares, of which the roots are of the form* $4n - 1$.

And, in general, the proposition is always reducible to the decomposition of a number into squares, and all the partial propositions that we have considered are included in the general form,

$$8\alpha\text{N} + (\alpha + 2)(\alpha - 2)^2 =$$
$$(2\alpha x - \alpha + 2)^2 + (2\alpha y - \alpha + 2)^2 + (2\alpha z - \alpha + 2)^2 + \&c.$$

the number of squares on the latter side of the equation being $(\alpha + 2)$.

CHAP. X.

On the different Scales of Notation, and their Application to the Solution of Arithmetical Problems.

PROP. I.

121. Every number N may be reduced to the form

$$N = ar^n + br^{n-1} + cr^{n-2} + \text{ \&c. } pr^2 + qr + w,$$

where r may be any number whatever, and a, b, c, &c., integers less than r.

For let N be divided by the greatest power of r contained in it, as r^n, and let the quotient be a, and remainder N′, so that

$$N = ar^n + N'.$$

Divide again N′ by the next lower power of r, as r^{n-1}, and let the quotient be b, which will be an integer or zero, according as N′ > or < r^{n-1}, and the remainder N″, whence

$$N = ar^n + br^{n-1} + N''.$$

Dividing again N″ by r^{n-2}, and supposing the quotient c, and remainder N‴, we have

$$N = ar^n + br^{n-1} + cr^{n-2} + N'''.$$

And by thus continually dividing the remainder by the next lower power of r, we shall be evidently brought finally to the form

$$N = ar^n + br^{n-1} + cr^{n-2} - - - pr^2 + qr + w;$$

in which expression, as a, b c, &c., are the quotients arising from the division of a number by the highest power of r contained in that number, it necessarily follows, that each of those coefficients, a, b, c, &c., is less than r. — Q. E. D.

Cor. If $r=10$, then a, b, c, &c., are the digits by which any number is expressed in our common method of notation; thus,

$$76034=7\,.\,10^4+6\,.\,10^3+0\,.\,10^2+3\,.\,10+4,$$
$$18461=1\,.\,10^4+8\,.\,10^3+4\,.\,10^2+6\,.\,10+1,$$

which form is always understood in enumerating the value of any number proposed; that is, we give to every digit a *local*, as well as its original or natural value: thus, in the number 76034, the second digit from the right is 3, but we consider it as representing 30, on account of its local situation, being in the second place from the right; in the same manner, the 6 represents 6000, and the 7 70000, so that the value of each digit is estimated according to its local situation and its original value, the former indicating the power of 10, and the latter the number of those powers that are intended to be expressed.

Cor. 2. It is evident, from the foregoing proposition, that a number may be in the same manner represented by any other value of the radix r, and hence arise the different scales of notation, which receive the following particular denominations according to the value of the radix r.

If $r=2$, it is termed the Binary scale.
$r=3$, - - - - Ternary.
$r=4$, - - - - Quaternary.

If $r = 5$, it is termed the Quinary.

$r = 6$, - - - - Senary.

$r = 10$, - - - - Denary, or common scale.

$r = 12$, - - - - Duodenary.

And since, by the foregoing proposition, a, b, c, &c., are always less than r, the radix of any system into which they enter; therefore it follows that for every scale we must have as many characters, including the cipher, as are equal to the number expressing the radix of the system. Thus, the only characters are, for the

Binary scale, - - 0, 1.

Ternary, - - - 0, 1, 2.

Quaternary, - - 0, 1, 2, 3.

Senary, - - - 0, 1, 2, 3, 4, 5.

Denary, or common scale, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

And hence it follows, that in the duodenary scale, we must have two additional characters for representing 10 and 11, and as these characters may be assumed at pleasure, we shall, in what follows, express 10 by the symbol ϕ, and 11 by π, whence the digits of the duodenary scale will be

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \phi, \pi.$$

PROP. II.

122. Having given the equation

$$\text{N} = ar^n + br^{n-1} + cr^{n-2} - - - pr^2 + qr + w,$$

in which N and r are given numbers, to find the unknown coefficients, a, b, c, &c., and the exponent n. Or, which is the same, to transform a

number from the denary to any other scale of notation.

It is evident that this may be done by proposition 1; namely, by dividing N successively by the highest power of r that is contained in it; but it is more readily performed by dividing N successively by r; thus, if

$$N = ar^n + br^{n-1} + cr^{n-2} - - - pr^2 + qr + w$$

be divided by r, the quotient will be

$$ar^{n-1} + br^{n-2} + cr^{n-3} - - - pr + q,$$

and the remainder w.

This last quotient being again divided by r gives for a new quotient

$$ar^{n-2} + br^{n-3} + cr^{n-4} - - - p,$$

and a remainder q. And this quotient, divided by r, gives a quotient

$$ar^{n-3} + br^{n-4} + cr^{n-5},$$

and a remainder p.

Whence it is evident, that the successive remainders will be the coefficients w, q, p, &c., or the digits that express any number in the scale of which r is the radix.

Ex. 1. Having given the equation

$$17486 = a.6^n + b.6^{n-1} + c.6^{n-2} - - - w,$$

to find a, b, c, &c. Or, which is the same, let it be proposed to convert 17486 from the common to the senary scale.

Here, by the foregoing proposition,

6)17486

6)2914 rem. = 2 = w

6)485 - - - 4 = q

6)80 - - - 5 = p

6)13 - - - 2 = c

6)2 - - - 1 = b

0 - - - 2 = a

Therefore, 17486, in the denary scale, is expressed by 212542 in the senary.

Ex. 2. Transform 1810 into both the binary and ternary scales.

2)1810	3)1810
2)905 rem. = 0	3)603 rem. = 1
2)452 - - - 1	3)201 - - - 0
2)226 - - - 0	3)67 - - - 0
2)113 - - - 0	3)22 - - - 1
2)56 - - - 1	3)7 - - - 1
2)28 - - - 0	3)2 - - - 1
2)14 - - - 0	0 - - - 2
2)7 - - - 0	
2)3 - - - 1	
2)1 - - - 1	
0 - - - 1	

Therefore, 1810 = 11100010010, in the binary scale; and 1810 = 2111001, in the ternary scale.

Ex. 3. Transform the two numbers, 844371 and 215855, from the denary to the duodenary scale.

12)844371		12)215855	
12)70364	rem. = 3	12)17987	rem. = $11 = \pi$
12)5863	- - - 8	12)1498	- - - $11 = \pi$
12)488	- - - 7	12)124	- - - $10 = \phi$
12)40	- - - 8	12)10	- - - $4 = 4$
12)3	- - - 4	0	- - - $10 = \phi$
0	- - - 3		

Hence $844371 = 348783$ and $215855 = \phi 4 \phi \pi \pi$, } in the duodenary scale.

And thus a number is readily transformed from the denary to any other system of which the radix is given, and hence we find 1000 is expressed in the following manner according to the value of the radix r.

If $r = 2$, $1000 = 1111101000$;
$r = 3$, $1000 = 1101001$;
$r = 4$, $1000 = 33220$;
$r = 5$, $1000 = 13000$;
$r = 6$, $1000 = 4344$;
$r = 7$, $1000 = 2626$;
$r = 8$, $1000 = 1750$;
$r = 9$, $1000 = 1331$;
$r = 10$, $1000 = 1000$;
$r = 11$, $1000 = 82\phi$;
$r = 12$, $1000 = 6\pi 4$.

Hence it is evident, as it is indeed from the nature of the subject under investigation, that the greater the radix is, the less will be the number of digits necessary for expressing any given number; but the operations of multiplication, division, &c., will be the more complex; and, therefore, in judging of the advantages and disadvantages of different systems, we ought to keep both these circumstances in view, as also a third, which is the number of prime divisors of the radix; and, on a just estimate of the whole, the radix 12 will be found preferable to any of the other systems: but on this subject we shall add a few remarks at the conclusion of this chapter.

PROP. III.

123. To transform a number from any other scale of notation to the denary, or common scale.

This proposition is the converse of the foregoing one, and it is readily effected by the reverse operation.

For let

$$ar^n + br^{n-1} + cr^{n-2} \text{ - - - } pr^2 + qr + w$$

represent a number in any known scale of notation, whose radix is r; then, since a, b, c, &c., are also known, we have only to collect the successive values of the different terms, and their sum will be the number transformed, as required.

Ex. 1. Transform 7184 from the duodenary to the common scale of notation.

First,

$$7184 = 7 \cdot 12^3 + 1 \cdot 12^2 + 8 \cdot 12 + 4.$$

Therefore, we have,

$$
\begin{aligned}
7 \cdot 12^3 &= 12096 \\
1 \cdot 12^2 &= 144 \\
8 \cdot 12 &= 96 \\
4 &= 4
\end{aligned}
$$

Duodenary $7184 = 12340$ Denary scale.

Ex. 2. Transform 1534 from the senary to the denary scale.

$$1534 = 1 \cdot 6^3 + 5 \cdot 6^2 + 3 \cdot 6 + 4$$

$$
\begin{aligned}
1 \cdot 6^3 &= 216 \\
5 \cdot 6^2 &= 180 \\
3 \cdot 6 &= 18 \\
4 &= 4
\end{aligned}
$$

Senary $1534 = 418$ in the common scale.

Cor. By means of the two foregoing propositions a number may be transformed from one scale of notation to another, neither of which is the denary, by first transforming it from the given scale to the common scale, and then into the particular one required.

PROP. IV.

124. In every scale of notation, whose radix is r, the sum of all the digits expressing any number, when divided by $r-1$, will leave the same remainder as the whole number divided by $r-1$; that is, if

$$N = ar^n + br^{n-1} + cr^{n-2} - - - pr^2 + qr + w,$$

then will $N \div (r-1)$, leave the same remainder, as

$$(a + b + c - - - p + q + w) \div (r-1).$$

For make $r-1=r'$, or $r=r'+1$, then

$$r^n \div (r-1) = (r'+1)^n \div r'$$

will leave a remainder 1, because every term of the expanded binomial $(r'+1)^n$ is divisible by r', except the last, which is 1; and, consequently, $(r'+1)^n \div r'$, or $r^n \div (r-1)$, will leave a remainder 1, and this property is entirely independent of the value of n; and hence it follows, that every power of r divided by $r-1$ will leave a remainder 1, or the powers r^n, r^{n-1}, r^{n-2}, &c., are all of the form $m(r-1)+1$; that is, $r^{n'} \doteqdot m(r-1)+1$, whatever integer value is given to n'.

And hence it follows, that

$$\begin{aligned}
ar^n &\doteqdot am(r-1)+a, \\
br^{n-1} &\doteqdot bm'(r-1)+b, \\
cr^{n-2} &\doteqdot cm''(r-1)+c, \\
&\text{\&c.} \qquad \text{\&c.} \\
pr^2 &\doteqdot pm'''(r-1)+p, \\
qr &\doteqdot qm^{iv}(r-1)+q, \\
w &\doteqdot \qquad\qquad w.
\end{aligned}$$

And, consequently,

$$\text{N} \doteqdot m^v(r-1)+(a+b+c+ \text{ - - - } p+q+w);$$

and, therefore, when divided by $r-1$, it will evidently leave the same remainder as the sum of its digits $(a+b+c$, &c. $w)$. — Q. E. D.

Cor. 1. Hence, if the sum of the digits in any system of notation be divisible by $r-1$, the whole number is divisible by $r-1$; therefore, in the common scale, if the digits of a number be divisible by 9, the number itself is divisible by 9, and if there be any remainder in the former, there will also be the same remainder in the latter; and if the sum of the digits be even, and divisible by 9, then

will the number itself be divisible by 18; because, if an even number be divisible by an odd number, it is divisible by double that number (cor., art. 5). And since 3 is a factor of 9, the same property that has been shown to belong to the number 9 belongs also to 3; namely, if the sum of digits of a number be divisible by 3, the number itself is divisible by 3, and if the sum be even also, then will the number be divisible by 6.

Cor. 2. It is upon this obvious principle that our rule for proving the truth of operations in multiplication, division, &c., is founded, by dividing by, or casting out the 9s contained in the two factors, and in the product; and what remains of this last ought to be equal to what remains of the product of the two former remainders divided by 9, if the work be right.

For let a and b represent any two factors, and make

$$a = 9n + a',$$

$$b = 9m + b'. \text{ Then}$$

$$ab = 9(9nm + ma' + nb') + a'b';$$

and, therefore, $ab \div 9$ leaves the same remainder as $a'b'$ divided by 9: but the remainder of $a \div 9$ is the same as the digits of a by 9, and the remainder of $b \div 9$ is the same as the digits of $b \div 9$, and the same of the product ab; and hence the reason of the rule.

The same is obviously true for any other system of notation, by taking the number next less than the radix for the divisor. Thus, for example, we have seen that $215855 = \phi 4 \phi \pi \pi$ in the duo-

denary scale, and $215855 \div 11$ leaves a remainder 2: but

$$\phi + 4 + \phi + \pi + \pi = 10 + 4 + 10 + 11 + 11 = 46,$$

which, divided by 11, gives also a remainder 2.

Suppose it was required to multiply $\phi 4 \phi \pi \pi$ by $\phi\phi 4$, the operation and proof would stand thus:

Operation.

```
  φ4φππ  rem. 2
    φφ4  rem. 2
  ------
 3577π8
8811π2
8811π2
--------
95088918 rem. 4
```

Proof by 11.

It is unnecessary to observe, that in this operation, as in all others in which the radix is r, we must in multiplying, dividing, &c., divide by the radix; that is, by 12 in the above example, and set down the overplus, instead of dividing by 10 and setting down the overplus, as is done in the common scale.

PROP. V.

125. In any scale of notation whose radix is r, the difference of the remainders of the sum of the 1st, 3d, 5th, &c., digits by $r+1$, and the sum of the 2d, 4th, 6th, &c., digits divided also by $r+1$, is equal to the remainder of the whole number divided by $r+1$.

Let

$$N = ar^n + br^{n-1} + cr^{n-2} - - - pr^2 + qr + w,$$

then, I say, the remainder of $(w + p + b \,\&\text{c.}) \div (r+1)$,

minus the remainder of $(q+c+a\ \&c.)\div(r+1)$, is equal to the remainder of $\text{N}\div(r+1)$.

For make $r+1=r'$, or $r=r'-1$, then it is evident that $\dfrac{(r'-1)^n}{r'}$ will leave a remainder $+1$, or -1, according as n is even or odd; for all the terms in the expanded binomial $(r'-1)^n$ are divisible by r', except the last, which is $+1$ or -1, according as n is even or odd, independently of any other value of n; and, therefore, $\dfrac{r^n}{r+1}$ will also leave the same remainder in the same cases; that is, every odd power of r is of the form $m(r+1)-1$, and every even power of r is of the form $n(r+1)+1$.

Therefore, in the above expression, we have

$$\begin{array}{lll} w & \doteq & +w, \\ qr & \doteq qm & (r+1)-q, \\ pr^2 & \doteq pn & (r+1)+p, \\ cr^{n-2} & \doteq cm' & (r+1)-c, \\ br^{n-3} & \doteq bn' & (r+1)+b, \\ ar^n & \doteq am'' & (r+1)-a, \\ \&c. & & \&c. \end{array}$$

And, consequently,

$$\text{N}\doteq m'''(r+1)+w-q+p-c+b-a;$$

and, therefore, when divided by $r+1$, it will leave the same remainder as

$(w-q+p-c+b-a)$ divided by $r+1$, or as $(w+p+b,\ \&c.)\div(r+1)-(q+c+a,\ \&c.)\div(r+1)$.

Q. E. D.

Cor. 1. Hence, in the common scale, if the sum of the digits in the odd places be equal to the sum of those in the even places, or if one exceed the

other by 11, or any multiple of 11, the whole number may be divided by 11.

Cor. 2. The above proposition furnishes us with another rule for proving the truth of operations in multiplication, division, &c., which, in the common scale of notation, the radix being 10, is as follows;

From the sum of the digits in the 1st, 3d, 5th, &c., places, subtract those in the 2d, 4th, 6th, &c., places in both factors, and in the product; also reserve the three remainders, when each of those differences is divided by 11; multiply the two former together, and cast out the 11s, which remainder ought to be equal to the remainder of the product, if the work be right. *Note*, if the sum of the 2d, 4th, &c., digits be greater than the sum of the 1st, 3d, &c., 11 must be added to the latter.

Thus, for example, to prove the truth of the multiplication in the following example:

741746	diff. of digits,	5
3462	diff. of digits,	8
1483492		11)40
4450476		
2966984		rem. 7
2225238		
2567924652	diff. of digits,	7

$$\begin{array}{ccc} & 7 & \\ 5 & \times & 8 \\ & 7 & \end{array}$$

This method, though not so easily expressed, is nearly as ready in practice as the rule by 9s; and, being independent of it, we may conclude, with a very considerable degree of certainty, that any example that proves right by both rules is really so in the operation. And the same rule is applicable

to any other radix by making that radix plus 1 the divisor.

Cor. 3. By means of cor. 1, art. 124, and cor. 1, art. 125, we are enabled to ascertain if a number be divisible by 3, 6, 9, 11, and 18, without attempting the operation, which is useful in finding the common measure of two numbers, reducing a fraction to its lowest terms, &c. And to these rules we may add the following; *viz.* If a number terminates with 5 or 0, it is divisible by 5 in both cases, and by 10 in the latter case; and if the two last digits of any number be divisible by 4, the whole number is divisible by 4; if the three last digits be divisible by 8, the number is divisible by 8; and, generally, if the n last digits be divisible by 2^n, the whole number is divisible by 2^n.

For every number ending in 5 or 0 is of one of the forms $10N + 5$ or $10N + 0$, both of which forms are evidently divisible by 5, and the latter by 10.

Again, every number may be expressed by $A \times 10^n + B$, where B represents the n last digits: thus, for example,

$$7846144 = 784614 \times 10 + 4 = 78461 \times 10^2 + 44 = 7846 \times 10^3 + 144, \ \&c.$$

And since 10 is divisible by 2, $10^n \div 2^n$; therefore, in the form $A \times 10^n + B$, which may represent any number whatever, $10^n \div 2^n$ and $B \div 2^n$ by hypothesis: therefore $A \times 10^n + B$ is divisible by 2^n, if B be so; that is, if the n last digits be divisible by 2^n.

PROP. VI.

126. To perform duodecimal operations by means of the duodenary scale of notation.

Transform the number of feet, if above 12,

into the duodenary scale, by art. 122, and set the inches and parts as decimals; then multiply as in common arithmetic, except carrying for every 12 instead of every 10, as in common operations. And, in the result, transform again the integral part of the product into the denary scale.

Ex. 1. Multiply 17 feet 3 inches 4 parts, by 19 feet 5 inches 11 parts.

Proof by 11.

$$\begin{array}{ccc} & 4 & \\ 2 & \times & 2 \\ & 4 & \end{array}$$

$$\begin{array}{rl}
15{\cdot}34 & = 17 \text{ ft. } \; 3 \text{ in. } \; 4'' \\
17{\cdot}5\pi & = 19 \qquad 5 \qquad 11 \\
\hline
13\phi08 & \\
7248 & \\
\phi0\pi4 & \\
1534 & \\
\hline
\end{array}$$

Answer, $240{\cdot}9688 = 336$ ft. $9'\ 6''\ 8'''\ 8^{iv}$.

Ex. 2. Find the solidity of a cube, whose side is 13 feet 7 inches 7 parts.

$$\begin{array}{rl}
11{\cdot}77 & = 13 \text{ ft. } \; 7 \text{ in. } \; 7'' \\
11{\cdot}77 & \\
\hline
7\pi51 & \\
7\pi51 & \\
1177 & \\
1177 & \\
\hline
135{\cdot}9\pi61 & \\
11{\cdot}77 & \\
\hline
9049867 & \\
9049867 & \\
1359\pi61 & \\
1359\pi61 & \\
\hline
\end{array}$$

Proof by 11.

$$\begin{array}{ccc} & 3 & \\ 5 & \times & 5 \\ & 3 & \end{array}$$

$$\begin{array}{ccc} & 4 & \\ 3 & \times & 5 \\ & 4 & \end{array}$$

$1571{\cdot}281417 = 2533$ ft $2'\ 8''\ 1'''\ 4^{iv}\ 1^{v}\ 7^{vi}$.

Remark. This method, which I first published in vol. xxv. of *Nicholson's Philosophical Journal,* appears to me to possess considerable advantage over the common rule, both on account of the facility of the operation, and the accuracy of the result, as, likewise, that it is thus submitted to proof, the same as common multiplication, which it is not possible to apply to the old method. The above examples are proved by 11, and they may also be proved by 13, according to rule, art. 125.

And in the same manner any other arithmetical operation, such as division, extracting the square root, &c., is performed with as much facility as in common numbers.

Ex. 1. Giving the area of a rectangle equal to 174 feet 11 inches, and its length 15 feet 7 inches; to find its breadth in feet, inches, &c.

174 ft. 11 in. $=126{\cdot}\pi$ and 15 ft. 7 in. $=13{\cdot}7$.

```
13·7)126·π(π·2841
     1235
     ----
      360
      272
      ---
      φφ0
      φ48
      ---
       540
       524
       ---
        180
        137
        ---
         45
```

Proof by 11.

```
   0
0  ╳  4
   0
```

The breadth is, therefore, 11 feet 2 inches 8′ 4″ 1‴.

As the above method of proving division is seldom or never given in books of arithmetic, it may not be amiss to say how it is effected, which is thus: from the sum of the digits in the dividend, take those in the remainder; then the remainder from the divisor and quotient, ought to be equal to that of the dividend thus reduced, if the work be right. The reason for which is evident, because the dividend minus the remainder may be considered as the product arising from the multiplication of the dividend and quotient.

Ex. 2. Given the breadth and area of a rectangle, equal to 24 feet 9 inches, and 971 feet 10 inches, to find its length.

24 ft. 9 in. $=20\cdot9$, and 971 ft. 10 in. $=68\pi\cdot\phi$

$$
\begin{array}{r}
20\cdot9)68\pi\cdot\phi(33\cdot323 \\
623 \\
\hline
68\phi \\
623 \\
\hline
670 \\
623 \\
\hline
490 \\
416 \\
\hline
760 \\
623 \\
\hline
139
\end{array}
$$

Proof by 11.

0
0 3
0

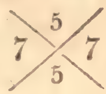
Therefore its length is 39 feet 3 inches 2′ 3″.

And the same principles are equally applicable to the extraction of the square root, as is evident by the following example:

Ex. 3. Having given the area of a square equal to 17 feet 4 inches 6′, required the length of its side.

	15·46(4·202ϕ
	14
82	146
2	144
8402	20000
2	14804
8404ϕ	73π800
	6π4404
	473π8

Proof.



Therefore the side is 4 feet 2 inches 0′ 2″ 10‴.

And thus may any other numerical operation be performed with nearly as much ease as in common arithmetic.

PROP. VII.

127. Every number less than 2^{n+1}, is compounded of some number of terms in the series,

$$1,\ 2,\ 2^2,\ 2^3,\ 2^4,\ 2^5,\ \&c.\ 2^n.$$

This is made evident by transforming any given number $N < a^{n+1}$ into the binary scale, which, from what has been observed at cor. 2, art. 121, will assume the form,

$$N = a.2^n + b.2^{n-1} + c.2^{n-2} - - - p.2^2 + q.2 + w;$$

where a, b, c, &c., are each less than 2, and consequently either 0 or 1; and as every number less than 2^{n+1} may be thrown into this form, therefore, with the above series, every number whatever,

within the assigned limits, may be compounded of some number of those terms.

Cor. 1. What is said in the above demonstration, not only proves the truth of the theorem, but also points out the method by which it is to be effected; and at the same time it is evident that there is only one way in which the selection can be made.

Cor. 2. In the above theorem, the greatest power of 2 is 2^n, and consequently the greatest number that can be formed is $2^{n+1}-1$; but, if the power of 2 be unlimited, so also will the number that may be compounded of those terms; that is, any number whatever may be compounded of the terms of the indefinite series, 1, 2, 2^2, 2^3, 2^4, &c.

Ex. Having a series of weights of

$$\overset{lb.}{1},\ \overset{lb.}{2},\ \overset{lb.}{4},\ \overset{lb.}{8},\ \overset{lb.}{16},\ \&c.,$$

it is required to ascertain which of them must be selected to weigh 1719 pounds.

First, 1719 in the binary scale is expressed by 11010110111: the weights therefore to be employed are,

$$\overset{lb.}{1}+\overset{lb.}{2}+\overset{lb.}{2^2}+\overset{lb.}{2^4}+\overset{lb.}{2^5}+\overset{lb.}{2^7}+\overset{lb.}{2^9}+\overset{lb.}{2^{10}}.$$

PROP. VIII.

128. Every number whatever may be formed by the sums and differences of the terms of the geometrical series, 1, 3, 3^2, 3^3, &c.

For, by transforming the given number N into the ternary scale of notation, it will assume the form,

$$N=a3^n+b3^{n-1}+c3^{n-2}\ \text{- - -}\ p3^2+q3+w;$$

where each of the coefficients, a, b, c, &c., is less than 3, and consequently they must be either 2, or 1, or 0. Now, in order to prove the truth of the theorem, it will be better to select a partial example, the reasoning on which will be evidently applicable to every other case. First, then, it is obvious, that, if no one of these coefficients be greater than 1, the question is resolved agreeably to the conditions of the proposition: we need, therefore, only consider the case, in which some one or more of the coefficients are equal to 2. Let, then,

$$\begin{cases} N = 3^n + 2.3^{n-1} + 0.3^{n-2} + 2.3^{n-3} + 3^{n-4} + 0.3^{n-5} + \\ \quad 2.3^{n-6}, \text{ \&c.} \end{cases}$$

And, since

$$3.3^{n-6} = 3^{n-5}, \text{ and } 3.3^{n-3} = 3^{n-2},\ 3.3^{n-1} = 3^n,$$

the above expression is the same as

$$(2.3^n + 3^{n-2} + 3^{n-4} + 3^{n-5}) - (3^{n-1} + 3^{n-3} + 3^{n-6}) =$$
$$(3^{n+1} + 3^{n-2} + 3^{n-4} + 3^{n-5}) - (3^n + 3^{n-1} + 3^{n-3} + 3^{n-6}) = N,$$

agreeably to the conditions of the proposition.—Q. E. D.

Remark. The latter part of the above demonstration is only for a particular case, but it is evident that the same reasoning will apply to any case, or even to the general form, but it would have only tended to lengthen and embarrass the demonstration, and at the same time would not have added to the certainty of the conclusion, for which reason it was thought better to proceed as above. This demonstration, like that in the foregoing proposition, has the advantage of pointing out the

method of solution, at the same time it proves the truth of the theorem, and, like that, also shows that there is only one way in which the theorem can be effected.

Cor. It appears from this theorem, that with a series of weights,

$$\overset{lb.}{1},\ \overset{lb.}{3},\ \overset{lb.}{3^2},\ \overset{lb.}{3^3},\ \overset{lb.}{3^4},\ \&c.,$$

any number of pounds whatever may be ascertained, by placing some of those weights in one scale and some in the other, when the case requires it, or only in one scale when the given weight is compounded of any number of those terms. The solution of which problem is readily deduced from the foregoing demonstration.

Ex. 1. Required in what manner the weights must be selected out of the foregoing series, to weigh 716 pounds.

First, 716 in the ternary scale is expressed by

$$\begin{array}{lrl} & 222112 & \\ \text{Add} & 1 & = 1 \\ \hline & 222120 & \\ \text{Add} & 10 & = 3 \\ \hline & 222200 & \\ \text{Add} & 100 & = 3^2 \\ \hline & 1000000 & = 3^6 \end{array}$$

therefore, $222112 = 3^6 - (3^2 + 3 + 1)$; that is, 3^6 must be placed in one scale, and the three weights $3^2 + 3 + 1$ in the other scale, with the body to be weighed.

Ex. 2. What weights out of the above

series must be selected, to ascertain a weight of 1319 pounds?

First, $1319 = 1210212$ in the ternary scale.

$$
\begin{array}{lrcl}
 & 1210212 & & \\
\text{Add} & 1 & = & 1 \\
\hline
 & 1210220 & & \\
\text{Add} & 10 & = & 3 \\
\hline
 & 1211000 & & \\
\text{Add} & 100000 & = & 3^5 \\
\hline
 & 2011000 & & \\
\text{Add} & 1000000 & = & 3^6 \\
\hline
 & 10011000 & = & 3^7 + 3^4 + 3^3
\end{array}
$$

And hence we conclude, that the weights $3^7 + 3^4 + 3^3$ must be put in one scale, and the weights $3^6 + 3^5 + 3 + 1$ in the other scale, with the body whose weight is to be ascertained.

These curious numerical problems are mentioned by Euler at page 253 of his *Analysis Infinitorum*, and the possibility of any weight being ascertained by such a system of weights is rigorously demonstrated; but the demonstration in the two foregoing problems is much simpler, and they have moreover the advantage of indicating the mode of solution, which is not attainable by Euler's method.

129. *Scholium.* Before we conclude this chapter, it will not be improper to make a few general observations on the comparative advantages and disadvantages of the different scales of notation, that have been the subject of our investigation. On this head, simplicity is evidently the first con-

sideration to be attended to, for in that alone consists the superiority of one system over another; but this ought to be estimated on two principles, *viz.* simplicity in arithmetical operations, and in arithmetical expressions: Leibnitz, by considering only the former, recommended the binary scale, which has certainly the advantage in all arithmetical operations, in point of ease; but this is more than counterbalanced by the intricacy of expression, on account of the multiplicity of figures necessary for representing a number of any considerable extent; thus we have seen (prop. ii. of this chapter), that 1000 in the binary scale would require ten places of figures, and to express 1000000 we must have twenty places, which would necessarily be very embarrassing, at the same time that all calculations would proceed very slow, on account of the number of figures that must be made to enter into them.

The next scale that has been recommended is the senary, which certainly possesses some important advantages: first, the operation with this system would be carried on with facility; the number of places of figures for expressing a number would not be very great; beside, that those quantities equivalent to our decimals, would be more frequently finite than they are in our system: for example, every fraction whose denominator is not some power of one of the factors of 10 is indefinite, and those only are finite that contain the powers of these factors; and it is exactly the same in every other scale of notation; namely, those fractions only are finite, that have denominators com-

pounded of the powers of the factors of the radix of that system; therefore, in the decimal scale only fractions of the form $\frac{a}{2^n 5^m}$ are finite, but in the senary scale the finite fractions are of the form $\frac{a}{2^n 3^m}$; and as there are necessarily more numbers of the form $2^n 3^m$, within any finite limit, than there are of the form $2^n 5^m$, it follows, that in a system of senary arithmetic, we should have more finite expressions for fractions than we have in the denary, and, consequently, on this head, the preference must be given to the senary system; and, indeed, the only possible objection that can be made to it is, that the operations would proceed a little slower than in the decimal scale, because in large numbers a greater number of figures must be employed to express them. This leads us to the consideration of the duodenary system of arithmetic, which, while it possesses all the advantages of the senary, in point of finite fractions, it is superior even to the decimal system for simplicity of expression; and the only additional burden to the memory is two characters for representing 10 and 11, for the multiplication table in our common arithmetic is generally carried as far as 12 times 12, although its natural limit is only 9 times 9, which is a clear proof that the mind is capable of working with the duodenary system, without any inconvenience or embarrassment; and hence, I think, we may conclude, that the choice of the denary arithmetic did not proceed from reflection and deliberation, but was the result of some cause

operating unseen and unknown on the inventor of our system; and it may, therefore, be considered as a fortunate circumstance, that for this accidental radix, that particular one should have been selected, which may be said to hold the second place in the scale of general utility.

All nations, both ancient and modern, with a very few exceptions, divide their numbers into periods of 10s, which singular coincidence of different people, entirely unconnected and unknown to each other, can only be attributed to some general physical cause, that operated equally on all, and which there is little doubt is connected with the formation of man; namely, his having ten fingers, by the assistance of which, in all probability, calculation, or at least numbering, was first effected.—See some ingenious remarks on this head, in *Montucla's Histoire des Mathematiques*, vol. i.

Our present scale of notation, however, though founded on this principle, was not the immediate consequence of this division, but was an improvement introduced a long time afterwards, as is evident from the arithmetic of the Greeks, who, notwithstanding they divided their numbers into periods of tens, had no idea of the present system of notation, the great and important advantage of which is, the giving to every digit a local, as well as its original or natural value, by means of which we are enabled to express any number, however large, with the different combinations of ten numerical symbols; whereas the Greeks, for want of this method, were under the necessity of employing *thirty-six* different characters, and with which, for

a long time, they were not able to express a number greater than 10000; it was, however, afterwards indefinitely extended by the improvements of *Archimedes*, *Apollonius*, *Pappus*, &c.

A Dissertation on the Notation and Arithmetic of the Greeks.

130. We have before observed, that the Greeks divided all their numbers into periods of tens, but that, for want of the happy idea of giving a local value to their numerical symbols, they were under the necessity of employing thirty-six characters, most of which were derived from their alphabet, and with which they contrived to render their arithmetic very regular, and as unembarrassing as such a number of symbols would admit.

Instead of our digits, - -	1,	2,	3,	4,	5,	6,	7,	8,	9,
they employed the characters - -	α,	β,	γ,	δ,	ε,	ϛ,	ζ,	η,	θ.
To represent -	10,	20,	30,	40,	50,	60,	70,	80,	90,
they made use of - -	ι,	κ,	λ,	μ,	ν,	ξ,	ο,	π,	ϟ.
For the hundreds they had - - -	ρ,	σ,	τ,	υ,	φ,	χ,	ψ,	ω,	ϡ.

But the thousands, 1000, 2000, &c., were represented by - ͵α, ͵β, ͵γ, ͵δ, ͵ε, ͵ϛ, ͵ζ, ͵η, ͵θ.

That is, they had recourse again to the characters of the simple units, with this difference only, that,

in order to distinguish them from the former, they placed a small *iota* or *dash* below the latter.

With these characters, it is evident that the Greeks could express any number under 10000, or a myriad. Thus,

991	was represented by	ϡϙα,
9999	- - - - - - -	͵θϡϙθ,
7382	- - - - - - -	͵ζτπβ,
8036	- - - - - - -	͵ηλϛ,
6420	- - - - - - -	͵ϛυκ,
4001	- - - - - - -	͵δα;

and so on for others: whence it is evident, that neither the order nor the number of characters had any effect in fixing the value of any number intended to be expressed; for 4001 is expressed by two characters, 6420 by three, and 7382 by four. Also the value of each of those expressions is the same, in whatever order they are placed; thus

͵θϡϙθ is the same as ϡϙ͵θθ, or as ϙ͵θθϡ;

and so on for any other possible combination; but as regularity tended in a great measure towards simplicity, they generally wrote the characters according to their value, as in the examples above.

In order to express any number of myriads, they made use of the letter M, placing above it the character representing the number of myriads they intended to indicate. Thus,

$$\overset{\alpha}{\mathrm{M}},\quad \overset{\beta}{\mathrm{M}},\quad \overset{\gamma}{\mathrm{M}},\quad \overset{\delta}{\mathrm{M}},\quad \&c.,$$

represented 10000, 20000, 30000, 40000. Thus,

also, $\overset{\lambda\zeta}{\mathrm{M}}$ expressed 370000, $\overset{,\delta\tau o\beta}{\mathrm{M}}$ = 43720000; and, generally, the letter M placed beneath any number, had the same effect as our annexing four ciphers.

This is the notation employed by Eutocius in his Commentaries on Archimedes, but it is evidently not very applicable to calculations.

Diophantus and Pappus represented their myriads by the two letters Mυ placed after the number, and hence, according to them, the above numbers would be written thus:

α.Mυ, β.Mυ, γ.Mυ, δ.Mυ, &c.

370000 = λζ.Mυ, and 43720000 = ͵δτοβ.Mυ.

Also 43728097 is expressed by ͵δτοβ.Mυ ͵ηϟζ,

And 99999999 - - - by ͵θϡϟθ.Mυ ͵θϡϟθ.

This notation in some measure resembles that which we employ for complex numbers, such as feet and inches, or pounds and shillings.

The same authors, however, employed a still more simple notation, by dropping the Mυ, and supplying its place with a point; thus, instead of

͵δτοβ.Mυ ͵ηϟζ, they wrote ͵δτοβ.͵ηϟζ; and for

͵θϡϟθ.Mυ ͵θϡϟθ, they wrote ͵θϡϟθ.͵θϡϟθ:

this last number, with the addition of unity, becomes $10000^2 = 100000000$, which was the greatest extent of the Greek arithmetic; and, for common purposes, it was quite sufficient, because their units of weight and measure, such as the talent and stade, were greater than our pound and foot. It was, therefore, only astronomers and geometers

who sometimes found an inconvenience in this limitation; thus, for example, Archimedes in his *Arinarius,* in order to express the number of grains of sand, that might be contained in a sphere that had for its diameter the distance of the fixed stars from the earth, found it necessary to represent a number which with our notation would require sixty-four places of figures; and in order to do this, he assumed the square myriad, or 100000000, as a new unit, and the numbers formed with these new units he called numbers of the second order; and thus he was enabled to express any number which in our notation requires sixteen figures: assuming again $(100000000)^2$ for a new unit, he could represent any number that requires in our scale twenty-four figures, and so on: so that by means of his numbers of the 8th order he could express the number in question, which, as we have said above, required sixty-four figures in our scale.

Hence, according to Archimedes, all numbers were separated into periods or orders of eight figures, which idea, as we are informed by Pappus, was considerably improved by Apollonius, who, instead of periods of eight places, and which were named by Archimedes octades, he reduced to periods of four figures; the first of which, on the left, were units, the second period myriads, the third double myriads, or numbers of the second order, and so on indefinitely.

In this manner Apollonius was able to write any number that can be expressed by our system of numeration; as, for example, if he had wished to represent the circumference of a circle, whose

diameter was a myriad of the ninth order, he would have written it thus:

γ. ͵αυιε. ͵θσξε. ͵γφπθ. ͵ϛϡλβ. ͵γωμϛ. ͵βχμγ.

3. 1415 9265 3589 7932 3846 2643.

͵γωλβ. ͵ϛϡν. ͵βωκδ.

3832 7950 2824.

Having thus given an idea of the Grecian notation for integer numbers, it remains to say a few words on their method of representing fractions. A small dash set on the right of a number, made of that number the denominator of a fraction, of which unity was the numerator; thus

$$\gamma' = \tfrac{1}{3},\ \delta' = \tfrac{1}{4},\ \xi\delta' = \tfrac{1}{64},\ \rho\kappa\alpha' = \tfrac{1}{121},\ \text{\&c.};$$

but the fraction $\frac{1}{2}$ had a particular character, as C, or <, C′, or K.

When the numerator is not unity, the denominator is placed as we set our exponents. Thus,

$$\iota\varepsilon^{\xi\delta},\ \text{represented}\ 15^{64},\ \text{or}\ \tfrac{15}{64};\ \text{and}$$

$$\zeta^{\rho\kappa\alpha},\ \text{represented}\ 7^{121},\ \text{or}\ \tfrac{7}{121}:\ \text{also}$$

$$\sigma\xi\gamma.\gamma\phi\mu\delta^{\lambda\gamma.\alpha\psi o\varsigma} = 2633544^{331776} = \tfrac{2633544}{331776}.$$

This last fraction is found in Diophantus, book 4, question 46.

As it was only our intention in this place to convey to the reader a connected and general idea of the notation of the Greeks, in order the better to estimate the value of the modern, or, as it is sometimes called, the Indian arithmetic, we have not entered into an explanation of their sexagesi-

mals employed by astronomers in the division of the circle, and of which ours is still a representative, as is evident from the following example:

$$0.\ \nu\theta'\ \eta''\ \iota\varsigma'''\ \iota\gamma^{iv}\ \iota\beta^{v}\ \lambda\alpha^{vi} =$$
$$0^{\circ}\ 59'\ 8''\ 17'''\ 13^{iv}\ 12^{v}\ 31^{vi}$$

131. It still remains for us to explain, by a few examples, the method that was employed by the ancients in order to perform the common rules of arithmetic, with this complicated system of notation, and must refer the curious reader, who wishes for more particular information, to an ingenious essay on this subject by Delambre, subjoined to the French translation of the Works of Archimedes, to which essay we are indebted for many of the foregoing and following remarks.

Example in Addition.

From Eutocius, Theorem 4, *of the Measure of the Circle.*

ωμζ. γϡκα	847 3921
ξ. ηυ	60 8400
ϡη. βτκα	908 2321

In this example the method of proceeding is so obvious, that it needs no explanation, being performed exactly as we do our compound addition of feet and inches, or pounds, shillings, and pence; but it is more simple on account of the constant ratio of ten between any character and the succeeding one.

Example in Subtraction.

Eutocius, Theorem 3, on the Measure of the Circle.

θ.͵γχλϛ	93636
β.͵γυ θ	23409
ϛ. σκϛ	70227

This example also is so simple, that the reader will find no difficulty in following the operation, by proceeding from right to left, as in our subtraction, which method seems so obviously advantageous and simple, that one can hardly conceive why the Greeks should ever proceed in the contrary way, although there are many instances which make it evident that they did, both in addition and subtraction, work from left to right.

In multiplication they most commonly proceeded in their operations from left to right, as we do in multiplication of algebra, and their successive products were placed without much apparent order, as is evident from the following examples; but as each of their characters retained always its own proper value, in whatever order they stood, the only inconvenience of this was, that it rendered the addition of them together a little more troublesome.

As it is burdensome to the memory to retain in mind the value of all the Greek characters, we have, for the ease of the reader, in the following examples, made the substitutions as below, by

which means their operations will be the more readily comprehended.

For $\alpha, \beta, \gamma, \delta$, &c. we write $1^\circ, 2^\circ, 3^\circ, 4^\circ$, &c.

$\iota, \kappa, \lambda, \mu$, &c. - - - - $1', 2', 3', 4'$, &c.

$\rho, \sigma, \tau, \upsilon$, &c. - - - - $1'', 2'', 3'', 4''$, &c.

${}_{,}\alpha, {}_{,}\beta, {}_{,}\gamma, {}_{,}\delta$, &c. - - - - $1''', 2''', 3''', 4'''$, &c.

And the myriads are represented by ^{m} placed over the number of them.

Thus, $1^\circ, 2^\circ, 3^\circ$, &c., have their proper value;

$1', 2', 3'$, &c. will represent 10, 20, 30, &c.

$1'', 2'', 3''$, &c. - - - - - - - 100, 200, 300, &c.

$1''', 2''', 3'''$, &c. - - - - - - - 1000, 2000, 3000, &c.

$1^{m}, 2^{m}, 3^{m}$, &c. will be so many myriads.

After which it will be extremely easy to follow the work in all the succeeding examples.

$\rho\nu\gamma$	$1''\ 5'\ 3$
$\rho\upsilon\gamma$	$1''\ 5'\ 3$
${}_{,}\alpha.\varsigma\tau$	$1^{m}.\ 5'''\ 3''$
${}_{,}\varepsilon{}_{,}\beta\phi\ \ \rho\nu$	$5'''\ 2'''\ 5''\ 1''\ 5'$
$\tau\rho\nu\theta$	$3''\ 1''\ 5'\ 9^\circ$
${}_{,}\beta.\gamma\upsilon\theta$	$2^{m}.\ 3'''\ 4''\ \ 9^\circ$

This example may be farther illustrated: thus, by beginning on the left hand, we have

$\rho \times \rho = \alpha$, or $100 \times 100 = 10000 = 1^m$

$\rho \times \nu = ͵\varepsilon$, or $100 \times 50 = 5000 = 5'''$

$\rho \times \gamma = \tau$, or $100 \times 3 = 300 = 3''$

Again,

$\nu \times \rho = ͵\varepsilon$, or $50 \times 100 = 5000 = 5'''$

$\nu \times \nu = ͵\beta\phi$, or $50 \times 500 = 2500 = 2'''\ 5''$

$\nu \times \gamma = \rho\nu$, or $50 \times 3 = 150 = 1''\ 5'$

Also,

$\gamma \times \rho = \tau$, or $3 \times 100 = 3''$

$\gamma \times \nu = \rho\nu$, or $3 \times 50 = 1\ 5'$

$\gamma \times \gamma = \nu$, or $3 \times 3 = 9^0$

Whence, by addition, we have evidently - - - - - - $\Big\}\ 2^m\ 3'''\ 4''\ 9^\circ$

The above example is exactly copied from Eutocius, and is sufficient to indicate the method that the Greeks employed in their multiplication, but it will not be amiss to present the reader with another example drawn from the same source.

$\phi o \alpha$	$5''\ 7'\ 1^\circ$
$\phi o \alpha$	$5''\ 7'\ 1^\circ$
$\underset{M}{\kappa\varepsilon}\ \underset{M}{\gamma}\ ͵\varepsilon\phi$	$25^m\ 3^m\ 5'''\ 5''$
$\underset{M}{\gamma}\ ͵\varepsilon\ ͵\delta$ϡ$o$	$3^m\ 5'''\ 4'''\ 9''\ 7'$
$\phi o \alpha$	$5''\ 7'\ 1^\circ$
$\underset{M}{\gamma\beta}\ ͵ϛ\mu\alpha$	$32^m\ 6'''\ 4'\ 1^\circ$

The division of the Greeks was still more intricate than their multiplication, for which reason it seems they generally preferred the sexagesimal division, and no example is left at length by any of those writers, except in the latter form; but these are sufficient to throw some light on the process they followed in the division of common numbers, and Delambre has accordingly supposed the following example:

Example in Division.

τλβ.͵γτκθ(͵αωκγ	$332^m\ 3'''\ 3''\ 2'\ 9^\circ(1'''\ 8''\ 2'\ 3^\circ$
ρπβ.͵γ ͵αωκγ	182 3 $1'''\ 8''\ 2'\ 3^\circ$
ρν. τκθ	150 0 3 2 9
ρμε.͵ηυ	145 8 4
δ.͵αϡκθ	4 1 9 2 9
γ.͵ϛυξ	3 6 4 6
͵ευξθ	5 4 6 9
͵ευξθ	5 4 6 9

This example will be found, on a slight inspection, to resemble our compound division, or that sort of division that we must necessarily employ, if we were to divide feet inches and parts, by similar denominations, which, together with the number of different characters that they made

use of, must have rendered this rule extremely laborious; and that for the extraction of the square root was of course equally difficult, the principle of which was the same as ours, except in the difference of the notation, though it appears that they frequently, instead of making use of the rule, found the root by successive trials, and then squared it in order to prove the truth of their assumption.

From the foregoing sketch of the notation and arithmetic of the Greeks, the reader will be able to form some estimate of the value and importance of the present system, which does perhaps as much honour to its inventor as any other discovery in the whole circle of the sciences, being that to which we must consider ourselves indebted for the many brilliant advances that have been subsequently made in the modern analysis and astronomy. Let any one compare the complicated multiplications of the ancients with the logarithmic operations of the moderns, and he will soon be convinced that he cannot set too high a value upon the discovery of our present system of arithmetic, which laid the foundation of that of logarithms, and many other of the most important improvements that have been made for facilitating calculations, and thereby extending the bounds of science to their utmost possible limits. He will also perceive how slow and progressive are the steps to knowledge, and by what imperceptible degrees we arrive towards perfection: from the first rude efforts of the Greeks, when their notation carried them no farther than to write down 10000, or a myriad, he will be able

to trace them through their several successive improvements, until it became indefinite like our own; first, by placing the character M under the number of myriads that they wished to represent, they extended it to 10000^2, or 100000000; but this position of the character being found inconvenient, was changed for Mυ, following the number it was before placed under; and this again was afterwards dropped for the more eligible form of a point, separating the myriads from the simple units: afterwards Archimedes invented his *octates,* or periods of eights, and thus gave an indefinite extent to the Grecian arithmetic, an idea that was considerably improved upon by Apollonius, by making the periods consist of only four places instead of eight, and dividing all numbers into orders of myriads. In this form it seems most astonishing, that he did not perceive the advantages of making the periods to consist of a less number of characters; for having by this means given a local value to his periods of four, it was only necessary to have done the same for the single digits, in order to have arrived at the system in present use, which is the more singular, as the use of the cipher was not unknown to the Greeks, being always employed in their sexagesimal operations, where it was necessary; and, consequently, the step between this improved form of their notation and that of the present system was extremely small, although the advantages of the latter, when compared with the former, were incalculably great.

It is much to be regretted, that we are ignorant to whom the brilliant invention of the decimal scale

is due; even the nation where it took its origin is not distinctly known, though it seems most probable to belong to the Indians, it being from these people that the Arabs first acquired their knowledge of it, which they carried into Spain about eight hundred years back, and whence it soon after circulated among the other European nations.

132. We shall here conclude our Numerical Investigations, adding, by way of praxis, the following propositions, the demonstrations of which depend upon the principles that have been the subject of inquiry in the preceding pages: and shall, in the following part, endeavour to show their application to the Indeterminate and Diophantine Analysis.

Miscellaneous Propositions.

1. The square of any prime number p, of the form $4n+1$, is of the form $25n^2+m^2$.

2. The sum of any number of consecutive cubes beginning with unity is a square, the root of which is equal to the sum of the roots of all the cubes.

3. The common difference of three integral square numbers in arithmetical progression cannot be an odd number.

4. There cannot be four square numbers in arithmetical progression.

5. The common difference of three square numbers in arithmetical progression cannot be a square number.

6. There cannot be three cube numbers in arithmetical progression.

7. There cannot be three square numbers in arithmetical progression either in integers or fractions, whose common difference is 1, 2, or 3.

8. If m be a prime number greater than 3, then will m^2-1 be divisible by 24.

9. In order to ascertain whether a given number a be a prime number, it is only necessary to solve the equation $a^2+y^2=z^2$, a minimum. Required proof.

10. No triangular number, except unity, is a cube number.

11. No triangular, except unity, can be equal to a pentagonal number.

12. The difference between a fraction and its reciprocal cannot be equal to a square.

13. No cube number, except 8, when increased by unity, can be a square.

14. The equation $2x^6+3y^6=z^6$ is impossible.

15. The equation $ax^6 \pm 7y^6=z^6$ is impossible for every value of a, except those that fall under one of the forms $7n$, or $7n+1$.

16. Every odd number prime to 5 is a divisor of any repetend digit, and the number of digits necessary to form the complete dividend will never exceed the number of units expressed by the divisor.

17. If r be a prime number, then will every prime divisor of the formula $a^n \pm 1$ be of the form $2nx+1$, except only the divisor $a+1$, when the ambiguous sign is $+$, and the divisor $a-1$ when that sign is $-$.

18. No square number can terminate with more than three equal effective digits.

19. The squares of all numbers composed of less than ten units, as 11, 111, 1111, &c., always have the form 1, 2, 3, 4, - - - 4, 3, 2, 1.

20. The equation $(x^2+y^2)^2+(x^2-y^2)^2=z^2$ is impossible.

21. The following equations are impossible:

1. $z^2y \pm y^2x = z^2$.
2. $a^3bx^4 \pm ab^3y^4 = z^2$.
3. $2a^3bx^4 \pm 2ab^3y^4 = z^2$.
4. $2a^3bx^4 \pm 4ab^3y^4 = z^2$.

Required the demonstrations.

22. Find the rational values of x and y in the two equations $2x^4+8y^4=z^2$, and $6x^4+54y^4=z^2$; or prove that there can be no such values.

23. Every even number is the sum of two prime numbers, and every odd number is the sum of three prime numbers. Required proof.

24. Every prime number of the form $3n+1$ is also of the form x^2+3y^2.

25. Let 1, 2, 3, 4, &c. - - - n, represent any continued product of n terms, and let p be any prime number whatever; then will the above product be divisible by such a power of p as has its exponent expressed by the sum of the integral parts of the fractions

$$\frac{n}{p}+\frac{n}{p^2}+\frac{n}{p^3}+\frac{n}{p^4}\ \&c.$$

Required proof.

26. What weights must be selected out of the single series 1, 3, 9, 27, 81, &c., to weigh 100100 pounds?

27. How many terms must be selected out of

the single series 1, 2, 4, 8, 16, &c., that their sum may be 17845?

28. Let N be any number whatever, and a the difference of N, and the next greater square; also b the difference of N, and the next less square; then will $N - ab$ be a complete square.

29. The expanded binomial

$$(1-1)^n = 1 - n + \frac{n(n-1)}{1\,.\,2} - \frac{n(n-1)(n-2)}{1\,.\,2\,.\,3} + \&c. = 0;$$

and if these terms be respectively multiplied by the series

1, 2, 3, 4, &c.

or by any power of these terms, except the *nth*, as

1^m, 2^m, 3^m, 4^m, &c.

the sum of all the terms thus produced is equal to zero. Required proof.

30. The continued product

$$1\,.\,2\,.\,3\,.\,4\,.\,\&c., (n-1)n =$$

$$n^n - n(n-1)^n + \frac{n(n-1)}{1\,.\,2}(n-2)^n -$$

$$\frac{n\,.\,(n-1)(n-2)}{1\,.\,2\,.\,3}(n-3)^n + \&c.$$

Required proof.

31. If a, b, and c, represent the three sides of a triangle, and C the angle contained by a and b, then, if

$$\begin{cases} a^2 + b^2 = c^2, \text{ the } \angle C = 90°; \\ a^2 + ab + b^2 = c^2, \text{ the } \angle C = 120°; \\ a^2 - ab + b^2 = c^2, \text{ the } \angle C = 60°. \end{cases}$$

PART II.

ON THE INDETERMINATE AND DIOPHANTINE ANALYSIS.

CHAP. I.

Continued Fractions, and their Application to various Problems.

DEFINITIONS.

133. 1. Every expression having the following form, *viz.*

$$\cfrac{1}{a+\cfrac{1}{b+\cfrac{1}{c+\cfrac{1}{d}+\ \&c.}}}$$

a, b, and c, being integers, is called a *Continued** *Fraction*; and it is *rational* or *irrational* according as the number of its terms is finite or infinite.

* Every expression of the more general form

$$\cfrac{a}{b\pm\cfrac{c}{d\pm\cfrac{e}{f\pm\ \&c.}}}$$

is a continued fraction; but in what follows we shall only have to consider those fractions that are of the form above given.

2. The series of fractions formed of the first term, the first two terms, the first three terms, &c., of any continued fraction, are called *Converging Fractions;* thus,

$$\frac{1}{a}; \qquad \frac{1}{a+\frac{1}{b}}; \qquad \frac{1}{a+\frac{1}{b+\frac{1}{c}}}; \quad \&c.$$

when reduced to the following forms,

$$\frac{1}{a}, \quad \frac{b}{ab+1}, \quad \frac{bc+1}{a(ab+1)+c}, \quad \&c.$$

are converging fractions.

PROPOSITION I.

134. To reduce any proposed fraction, $\frac{\text{M}}{\text{N}}$, to the form of a continued fraction.

Let $\text{N} > \text{M}$; and suppose that N, when divided by M, gives a quotient a, and remainder P; then we have

$$\frac{\text{N}}{\text{M}} = a + \frac{\text{P}}{\text{M}}, \text{ and } \frac{\text{M}}{\text{N}} = \frac{1}{a+\frac{\text{P}}{\text{M}}}.$$

Dividing in the same manner M by P, and supposing the quotient b, and remainder Q, we have, in the same manner,

$$\frac{\text{M}}{\text{P}} = b + \frac{\text{Q}}{\text{P}}, \text{ and } \frac{\text{P}}{\text{M}} = \frac{1}{b+\frac{\text{Q}}{\text{P}}};$$

$$\frac{\text{P}}{\text{Q}} = c + \frac{\text{R}}{\text{Q}}, \text{ and } \frac{\text{Q}}{\text{P}} = \frac{1}{c+\frac{\text{R}}{\text{Q}}};$$

$$\frac{Q}{R}=d+\frac{S}{R}, \text{ and } \frac{R}{Q}=\cfrac{1}{d+\cfrac{S}{R}};$$

&c. &c. &c.

where a, b, c, &c., are the quotients arising from dividing, successively, N by M, M by P, P by Q, &c. And if now we substitute for the fractions $\frac{M}{N}$, $\frac{P}{M}$, $\frac{Q}{P}$, &c., their respective values, found as above, we obtain the following expression:

$$\frac{M}{N}=\cfrac{1}{a+\cfrac{P}{M}}=\cfrac{1}{a+\cfrac{1}{b+\cfrac{Q}{P}}}=\cfrac{1}{a+\cfrac{1}{b+\cfrac{1}{c+\cfrac{R}{Q}}}}:$$

and, consequently, the fraction $\frac{M}{N}$ is reduced to a continued fraction as required.

135. We are thus furnished with a very simple practical method of performing this reduction, in all such cases; *viz.* divide the denominator by the numerator, then the divisor by the remainder, and so on, as in finding the greatest common measure of two numbers; and the successive quotients will be the denominators of the fractions, above represented by a, b, c, &c.

Note. If the numerator be greater than the denominator, the continued fraction will be preceded by an integer.

Ex. 1. Reduce $\frac{1171}{9743}$ to a continued fraction.

```
1171)9743(8
     9368
     ----
      375)1171(3
          1125
          ----
            46)375(8
               368
               ---
                 7)46(6
                   42
                   --
                    4)7(1
                      4
                      -
                      3)4(1
                        3
                        -
                        1)3(3
                          3
                          -
                          0
```

Consequently the fraction proposed becomes

$$\frac{1171}{9743}=\cfrac{1}{8+\cfrac{1}{3+\cfrac{1}{8+\cfrac{1}{6+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{3}}}}}}},$$

which is therefore reduced to a continued fraction as was required.

Ex. 2. Reduce $\frac{743}{611}$ to a continued fraction.

611)743(1
611

132)611(4
528

83)132(1
83

49)83(1
49

34)49(1
34

15)34(2
30

4)15(3
12

3)4(1
3

1)3(3
3

And therefore we have for the required fraction

$$\frac{743}{611}=1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{3}}}}}}}},$$

which is preceded by an integer, as stated in the foregoing note.

Remark. We call the integers a, b, c, d, &c., obtained in the foregoing operation, *Quotients*, being the results of successive divisions; and each of these, with its depending fraction, as $a+\frac{P}{M}$, $b+\frac{Q}{R}$, $c+\frac{R}{Q}$, &c., is called a *Complete Quotient.*

PROP. II.

136. To transform a given continued fraction to a series of converging fractions.

Let
$$\cfrac{1}{a+\cfrac{1}{b+\cfrac{1}{c+\cfrac{1}{d+\text{ \&c.}}}}}$$

be any continued fraction: it is required to transform it to a series of converging fractions.

This is in fact performed by the common rules for the reduction of complex fractions to simple ones; thus

$$\frac{1}{a}=\frac{1}{a}$$

$$\cfrac{1}{a+\cfrac{1}{b}}=\cfrac{1}{\cfrac{ab+1}{b}}=\frac{b}{ab+1}$$

$$\cfrac{1}{a+\cfrac{1}{b+\cfrac{1}{c}}}=\cfrac{1}{a+\cfrac{1}{\cfrac{bc+1}{c}}}=\cfrac{1}{a+\cfrac{c}{bc+1}}=$$

$$\cfrac{1}{\cfrac{a(bc+1)+c}{bc+1}}=\frac{bc+1}{a(bc+1)+c}=\frac{bc+1}{(ab+1)c+a}.$$

And in the same manner we find

$$\cfrac{1}{a+\cfrac{1}{b+\cfrac{1}{c+\cfrac{1}{d}}}} = \frac{(bc+1)d+b}{\{(ab+1)c+a\}d+ab+1}$$

But this reduction, when there are many terms in the continued fraction, becomes very embarrassing, and at the same time unnecessary; for, from what has been already done, a very obvious law of formation discovers itself, in order to render which the more manifest, let us resume our foregoing results, making also the successive substitutions as below; *viz.*

$$\frac{1}{a} \text{ - - - } = \frac{1}{a} \text{ - - - - - - } = \frac{p^\circ}{q^\circ}$$

$$\cfrac{1}{a+\cfrac{1}{b}} \text{ - } = \frac{b}{ab+1} \text{ - - - - } = \frac{p'}{q'}$$

$$\cfrac{1}{a+\cfrac{1}{b+\cfrac{1}{c}}} = \frac{bc+1}{(ab+1)c+a} \text{ - - - } = \frac{p''}{q''}$$

$$\cfrac{1}{a+\cfrac{1}{b+\cfrac{1}{c+\cfrac{1}{d}}}} = \frac{(bc+1)d+b}{\{(ab+1)c+a\}d+ab+1} = \frac{p'''}{q'''}$$

Now here it is obvious, that

$$\begin{array}{lll}
p^\circ = 1 & \text{- - - -} & q^\circ = a \\
p' = bp^\circ & \text{- - -} & q' = bq^\circ + 1 \\
p'' = cp' + p^\circ & \text{- -} & q'' = cq' + q^\circ \\
p''' = dp'' + p' & \text{- -} & q''' = dq'' + q' \\
p^{\text{iv}} = ep''' + p'' & \text{- -} & q^{\text{iv}} = eq''' + q'';
\end{array}$$

and thus the successive terms of the series of converging fractions may be obtained as far as we please, by means of the given quantities a, b, c, &c.; these terms being

$$\frac{p^{\circ}}{q^{\circ}},\ \frac{p'}{q'},\ \frac{p''}{q''},\ \frac{p'''}{q'''},\ \text{\&c.}$$

137. Hence we have the following very easy method of reducing any continued fraction to a series of converging fractions.

Write all the denominators of the successive terms of the continued fraction in a line, thus

$$a,\ b,\ c,\ d,\ e,\ \text{\&c.};$$

then the first fraction will have unity for its numerator, and the first term, a, for its denominator; the second will have the second term, b, for its numerator, and for its denominator $ab+1$; and the numerators of all the succeeding fractions will be found, by multiplying the numerator last found by the corresponding term in the above series, and adding to the product the preceding numerator; and the denominators are obtained in exactly the same manner, as is evident from the foregoing proposition: thus,

$$a,\quad b,\quad c,\qquad d,\qquad\qquad e,\quad \text{\&c.}$$

$$\frac{1}{a},\ \frac{b}{ab+1},\ \frac{bc+1}{(ab+1)c+a},\ \frac{(bc+1)d+b}{\{(ab+1)c+a\}d+(ab+1)},\quad \text{\&c.}$$

the last term of which series will be the original fraction first proposed.

Ex. 1. Transform the continued fraction

$$\frac{1}{7+\frac{1}{6+\frac{1}{5+\frac{1}{2+\frac{1}{3}}}}}$$

to a series of converging fractions;

$$\begin{array}{llllll} \text{Denominators,} & 7, & 6, & 5, & 2, & 3, \\ \text{Conv. fractions,} & \frac{1}{7}, & \frac{6}{43}, & \frac{31}{222}, & \frac{68}{487}, & \frac{235}{1683}, \end{array}$$

the series required.

138. It is also obvious, that we may thus find the series of fractions converging towards any given quantity, without reducing it first to the continued form. For we have seen (art. 135), that the denominators a, b, c, &c., of the terms of any continued fractions, are the quotients obtained from finding the common measure of the two terms of the given fraction; and, therefore, having found these quotients, we may immediately ascertain the series of converging fractions, without any intermediate step; in fact, the consideration of any quantity under the form of a continued fraction is entirely useless, otherwise than as it leads us to the properties, and the law of formation, of the converging fractions; for it is in this form only, that these expressions are at all applicable to any useful purposes.

Ex. 2. Find the series of fractions converging towards the given fraction $\frac{39}{187}$.

$$\begin{array}{l}
39)187(4 \\
\quad 156 \\
\quad \overline{\;\;31)39(1} \\
\qquad\quad 31 \\
\qquad\quad \overline{\;8)31(3} \\
\qquad\qquad\; 24 \\
\qquad\qquad\; \overline{\;7)8(1} \\
\qquad\qquad\quad\;\; 7 \\
\qquad\qquad\quad\;\; \overline{1)7(7} \\
\qquad\qquad\qquad\;\; 7
\end{array}$$

Quotients, $4, \; 1, \; 3, \; 1, \; 7;$

Conv. frac. - - $\frac{1}{4}, \; \frac{1}{5}, \; \frac{4}{19}, \; \frac{5}{24}, \; \frac{39}{187},$

which is the series of converging fractions required.

139. If now any series of quotients derived from the fraction $\frac{M}{N}$ be represented by

$$a, \; b \; c, \; \&c., \; v, \; u, \; w, \; \&c.;$$

and - - $\frac{a}{1}$, - - - $\frac{p^{\circ}}{p^{\circ}}, \; \frac{p'}{q'}, \; \frac{p''}{q''}$, &c.,

be the corresponding converging fractions; then, from what has been shown above,

$$\frac{p''}{q''} = \frac{up' + p^{\circ}}{uq' + q^{\circ}};$$

and if instead of u, we substitute the complete quotient corresponding with it, as $u+\frac{y}{z}$ (*remark*, page 266), we shall have the original fraction

$$\frac{M}{N}=\frac{p'(u+\frac{y}{z})+p^{\circ}}{q'(u+\frac{y}{z})+p^{\circ}}.$$

For it is evident, referring to the original form,

$$\frac{M}{N}=\cfrac{1}{a+\cfrac{1}{b+\text{ \&c. }\cfrac{1}{t+\cfrac{1}{v+\cfrac{1}{u+\frac{y}{z}}}}}},$$

that, by stopping at any particular quotient, and annexing thereto the remainder $\frac{y}{z}$, we have the precise value of the original fraction, as will be still more obvious by turning to the form at art. 134.

Let now $u+\frac{y}{z}=u'$, then the above becomes

$$\frac{M}{N}=\cfrac{1}{a+\text{ \&c. }\cfrac{1}{t+\cfrac{1}{v+\cfrac{1}{u'}}}};$$

and as the order of formation of the converging fractions does not depend upon any particular values of these quotients, it is obvious that the same law will obtain for the complete quotient u' as for any other; supposing, therefore,

$$\left.\begin{matrix}\dfrac{1}{a+} \;\&c.\; \dfrac{1}{t}\end{matrix}\right\} = \frac{p^{\circ}}{q^{\circ}} \text{ and } \left.\begin{matrix}\dfrac{1}{a+} \;\&c.\; \dfrac{1}{t+\dfrac{1}{v}}\end{matrix}\right\} = \frac{p'}{q'},$$

we shall have, on the principles of art. 138,

$$\left.\begin{matrix}\dfrac{1}{a+} \;\&c.\; \dfrac{1}{t+\dfrac{1}{v+\dfrac{1}{u'},}}\end{matrix}\right\} = \frac{p'u'+p^{\circ}}{q'u'+q^{\circ}}, \text{ or}$$

$$\frac{\text{M}}{\text{N}} = \frac{p'(u+\frac{y}{z})+p^{\circ}}{q'(u+\frac{y}{z})+q^{\circ}}. \qquad \text{Q. E. D.}$$

For example, in the reduction of $\frac{711}{953}$, if we stop at any term as below,

```
711)953(1
    711
    ---
    242)711(2
        484
        ---
        227)242(1 15/227 complete quotient
            227
            ---
             15
```

we shall have the following result:

Quotients, - - $1,\; 2,\; 1\frac{15}{227}$

Conv. frac. - - $\frac{1}{1},\; \frac{2}{3},\; \dfrac{2(1+\frac{15}{227})+1}{3(1+\frac{15}{227})+1} =$

$\dfrac{2(227+15)+227}{3(227+15)+227} = \dfrac{717}{953}$, the original fraction;

and the same has place for every complete quotient, as is evident from the preceding demonstration.

PROP. III.

140. If $\frac{p^\circ}{q^\circ}$ and $\frac{p'}{q'}$ be any two consecutive terms in a series of fractions converging towards $\frac{M}{N}$; then will

$$p^\circ q' - p' q^\circ = \pm 1;$$

the ambiguous sign being $+$ when $\frac{p^\circ}{q^\circ} > \frac{M}{N}$, and $-$ when $\frac{p^\circ}{q^\circ} < \frac{M}{N}$.

For let

$$\begin{cases} a, & b, & c, & \&c. & v, & u, & w, & & \&c. \\ \frac{1}{a}, & \frac{b}{ab+1}, & & \&c. & \frac{p^\circ}{q^\circ}, & \frac{p'}{q'}, & \frac{p''}{q''}, & \frac{p'''}{q'''}, & \&c. \end{cases}$$

represent any series of quotients, with their corresponding fractions; then (art. 139) we have

$$p''' = p''w + p', \text{ and } q''' = q''w + q'; \text{ or}$$

$$\frac{p''' - p'}{p''} = \frac{q''' - q'}{q''} = w;$$

and, therefore,

$$p'''q'' - p'q'' = p''q''' - p''q', \text{ or}$$
$$p'''q'' - p''q''' = p'q'' - p''q'.$$

And, in the same manner, since

$$p'' = p'u + p^\circ, \text{ and } q'' = q'u + q^\circ, \text{ we have}$$

$$\frac{p'' - p^\circ}{p'} = \frac{q'' - q^\circ}{q'}; \text{ whence}$$

$$\therefore\ p''q' - p^\circ q' = p'q'' - p'q^\circ, \text{ or}$$

$$p''q' - p'q'' = p^\circ q' - p'q^\circ; \text{ that is,}$$

$$p'''q'' - p''q''' = p'q'' - p''q' = p'q^\circ - p^\circ q';$$

or the successive differences between the products of each numerator and consecutive denominator, and the product of the denominator and the numerator of the same fractions, are equal (abstracting from their signs); but the difference $(ab+1)-ab$, that is of the first two fractions, is 1, and since the differences are all equal, they are each equal to 1; and, therefore, $p^\circ q' - p'q^\circ = \pm 1$.

But when $\frac{p^\circ}{q^\circ} > \frac{\text{M}}{\text{N}}$, then $\frac{p'}{q'} < \frac{\text{M}}{\text{N}}$; and, consequently, $\frac{p^\circ}{q^\circ} > \frac{p'}{q'}$, and $\frac{p^\circ q'}{q^\circ q'} > \frac{p'q^\circ}{q^\circ q'}$; and, therefore,

$$p^\circ q' > p'q^\circ; \text{ that is, } p^\circ q' - p'q^\circ = +1.$$

And, for the same reason, if $\frac{p^\circ}{q^\circ} < \frac{\text{M}}{\text{N}}$, then we have $p^\circ q' - p'q^\circ = -1$. — Q. E. D.

141. It is this property of converging fractions, that renders them so useful in the solution of all indeterminate equations of the first degree; for every equation of this kind has its solution depending upon that of the equation,

$$ax - by = \pm 1,$$

as will be shown in the next chapter.

Now the solution of $ax - by = \pm 1$ is obtained by finding the series of fractions converging towards $\frac{a}{b}$; and assuming for x and y the terms of that

fraction, immediately preceding $\frac{a}{b}$, as is evident from the foregoing proposition.

Ex. 1. Find x and y in the indeterminate equation

$$16x - 41y = 1.$$

First,

$$\begin{array}{l} 16)41(2 \\ \quad\;\; 32 \\ \quad\;\; \overline{9)16(1} \\ \qquad\quad 9 \\ \qquad\quad \overline{7)9(1} \\ \qquad\qquad 7 \\ \qquad\qquad \overline{2)7(3} \\ \qquad\qquad\;\; 6 \\ \qquad\qquad\;\; \overline{1)2(2} \\ \qquad\qquad\qquad 2 \end{array}$$

Quotients, $2, \; 1, \; 1, \; 3, \; 2,$

Conv. frac. $\frac{1}{2}, \; \frac{1}{3}, \; \frac{2}{5}, \; \frac{7}{18}, \; \frac{16}{41},$

Whence we have $x = 18$, and $y = 7$, which gives

$$16x - 41y = 1, \text{ or } 16 \,.\, 18 - 41 \,.\, 7 = 1.$$

And it is obvious, that we shall have the same result if we take $x = 18 \pm 41m$, and $y = 7 \pm 16m$; m being indeterminate for this substitution gives also

$$16(18 \pm 41m) - 41(7 \pm 16m) = 1;$$

and by means of the indeterminate quantity m, an infinite number of values of x and y may be obtained, that will answer the conditions of the equation.

If the given indeterminate equation had been

$$ax - by = -1,$$

then we must have taken

$$x = 41m - 18, \text{ and } y = 16m - 7,$$

which gives

$$16(41m - 18) - 41(16m - 7) = -1;$$

where the indeterminate quantity m is also the means of furnishing an infinite number of solutions to the equation $ax - by = -1$.

But as this subject belongs properly to the next chapter, we must dismiss it for the present, and continue our investigation of continued fractions.

PROP. IV.

142. If $\frac{p^\circ}{q^\circ}$, $\frac{p'}{q'}$, $\frac{p''}{q''}$, $\frac{p'''}{q'''}$, &c. be a series of fractions converging towards any given fraction $\frac{\text{M}}{\text{N}}$, then will these fractions be alternately greater and less than the given fraction; but each approaches nearer to the true value of the original, than the one which precedes it.

The first part of the proposition is evident from considering the law of formation of these fractions: for let

$$\frac{\text{M}}{\text{N}} = \cfrac{1}{a + \cfrac{1}{b + \cfrac{1}{c + \cfrac{1}{d} \, \&c.}}};$$

hen it is obvious, that $\frac{1}{a} > \frac{\text{M}}{\text{N}}$; because, in order

to have the exact value, we must add a certain quantity to the denominator a (equal to all the other part of the expression): and

$$\frac{1}{b} > \left\{ \frac{1}{b + \frac{1}{c + \frac{1}{d}}} \right.$$

for the same reason; whence it follows, that

$$\left. \frac{1}{a + \frac{1}{b}} \right\} < \frac{\text{M}}{\text{N}};$$

because, in adding $\frac{1}{b}$ to the denominator a, we make it too great, and, consequently, the fraction too small; and in the same way we find that

$$\left. \frac{1}{a + \frac{1}{b + \frac{1}{c}}} \right\} > \frac{\text{M}}{\text{N}};$$

and so on alternately. But, by article 136,

$$\frac{1}{a}; \qquad \frac{1}{a + \frac{1}{b}}; \qquad \frac{1}{a + \frac{1}{b + \frac{1}{c}}}; \quad \&c.$$

are the successive terms of the converging series, being equal to

$$\frac{p^\circ}{q^\circ}, \ \frac{p'}{q'}, \ \frac{p''}{q''}, \ \&c.;$$

and, therefore, these terms are alternately greater and less than the original fraction; and hence it follows, that the value of this last is always contained between any two consecutive terms of the converging series.

Now, in order to demonstrate the latter part of the proposition, let us consider the difference between any converging fraction, and the original one to which it is an approximation. For which purpose, let $\frac{p^\circ}{q^\circ}$ be the fraction immediately preceding $\frac{p}{q}$; and let $u+\frac{x}{z}$ be the complete quotient, corresponding to $\frac{p}{q}$; also, for the sake of simplifying, put

$$u+\frac{x}{z}=u',$$

then we shall have, the same as in art. 139,

$$\frac{\text{M}}{\text{N}}=\frac{pu'+p^\circ}{qu'+q^\circ};$$

from which we derive

$$\frac{\text{M}}{\text{N}}-\frac{p}{q}=\frac{p^\circ q-pq^\circ}{q(qu'+q^\circ)}=\frac{\mp 1}{q(qu'+q^\circ)}; \text{ and}$$

$$\frac{\text{M}}{\text{N}}-\frac{p^\circ}{q^\circ}=\frac{(pq^\circ-p^\circ q)u'}{q^\circ(qu'+q^\circ)}=\frac{\pm u'}{q^\circ(qu'+q^\circ)}.$$

Whence we draw the following conclusions:

1. That $\frac{\text{M}}{\text{N}}-\frac{p}{q}$, and $\frac{\text{M}}{\text{N}}-\frac{p^\circ}{q^\circ}$, have always different signs.

2. That the difference $\frac{\text{M}}{\text{N}}-\frac{p}{q}<\frac{1}{q^2}$; which may therefore always be represented by $\frac{d}{q^2}$ when $d<1$.

3. That $\frac{\text{M}}{\text{N}}-\frac{p}{q}$ is less, abstracting from its

sign, than $\frac{M}{N} - \frac{p^\circ}{q^\circ}$; the former being equal to $\frac{1}{q(qu' + q^\circ)}$, and the latter to $\frac{u'}{q^\circ(qu' + q^\circ)}$; that is,

$$\frac{M}{N} - \frac{p}{q} = \frac{1}{q} \times \frac{1}{qu' + q^\circ}, \text{ and}$$

$$\frac{M}{N} - \frac{p^\circ}{q^\circ} = \frac{u'}{q^\circ} \times \frac{1}{qu' + q^\circ}.$$

Now $u' = u + \frac{x}{z}$; and, therefore, $u' > 1$, and $q > q^\circ$, from the nature of these fractions; much more, then, is $\frac{u'}{q^\circ} > \frac{1}{q}$. Since, therefore, the difference between any converging fraction and the original is less than the difference between the preceding one and the original, it follows, that the value of any fraction $\frac{p}{q}$ approaches nearer to that of $\frac{M}{N}$ than any one which precedes it.

PROP. V.

143. To convert the square root of any given number N (not a square) into a continued fraction, and thence to a series of converging fractions, approximating towards the $\sqrt{N}$.

It is evident, in the first place, that this series must be infinite; because the square root of a number not a square cannot be expressed by any rational fraction (art. 18); but we shall find, that the quotient, whence the series of converging fractions are derived, will be periodical; and, therefore, the extraction may be carried on at pleasure. The

method of transformation, in this case, will be better shown by a partial, than by a general example; and we shall, therefore, first extract the square root of 19, and afterwards show the application of the same method to the extraction of any quantity of the form $\frac{\sqrt{N}+M}{P}$; N, M, and P, being integers.

Extraction of $\sqrt{19}$ *in Continued Fractions.*

$$\sqrt{19} = 4 + \frac{\sqrt{19}-4}{1} = 4 + \frac{3}{\sqrt{19}+4} = 4 + \frac{1}{\frac{\sqrt{19}+4}{3}};$$

$$\frac{\sqrt{19}+4}{3} = 2 + \frac{\sqrt{19}-2}{3} = 2 + \frac{5}{\sqrt{19}+2} = 2 + \frac{1}{\frac{\sqrt{19}+2}{5}};$$

$$\frac{\sqrt{19}+2}{5} = 1 + \frac{\sqrt{19}-3}{5} = 1 + \frac{2}{\sqrt{19}+3} = 1 + \frac{1}{\frac{\sqrt{19}+3}{2}};$$

$$\frac{\sqrt{19}+3}{2} = 3 + \frac{\sqrt{19}-3}{2} = 3 + \frac{5}{\sqrt{19}+3} = 3 + \frac{1}{\frac{\sqrt{19}+3}{5}};$$

$$\frac{\sqrt{19}+3}{5} = 1 + \frac{\sqrt{19}-2}{5} = 1 + \frac{3}{\sqrt{19}+2} = 1 + \frac{1}{\frac{\sqrt{19}+2}{3}};$$

$$\frac{\sqrt{19}+2}{3} = 2 + \frac{\sqrt{19}-4}{3} = 2 + \frac{1}{\sqrt{19}+4} = 2 + \frac{1}{\frac{\sqrt{19}+4}{1}};$$

$$\frac{\sqrt{19}+4}{1} = 8 + \frac{\sqrt{19}-4}{1} = \&c.$$

And here, since we have obtained the same ex-

pression as we began with, we may discontinue our extraction; as the quotients 4; 2, 1, 3, 1, 2, 8; 2, 1, 3, 1, 2, 8; 2, 1, &c.; must necessarily recur again in the same order, *ad infinitum.*

Now if we substitute for the fractions

$$\frac{\sqrt{19}+4}{3},\quad \frac{\sqrt{19}+2}{5},\quad \frac{\sqrt{19}+3}{2},\quad \frac{\sqrt{19}+2}{3},\ \&c.$$

their respective values, as found in the foregoing operation, we shall have

$$\sqrt{19}=4+\cfrac{1}{\cfrac{\sqrt{19}+4}{3}}=4+\cfrac{1}{2+\cfrac{1}{\cfrac{\sqrt{19}+2}{5}}}=$$

$$4+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{\cfrac{\sqrt{19}+3}{2}}}}=4+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{8+\&c.}}}}}}$$

and, therefore, the square root of 19 has been transformed into a continued fraction, as was required: and hence it is obvious that the same may be converted into a series of converging fractions, as in art. 136; thus,

Quotients,	4,	2,	1,	3,	1,	2,	8,	
Conv. frac.	$\frac{4}{1}$,	$\frac{9}{2}$,	$\frac{13}{3}$,	$\frac{48}{11}$,	$\frac{61}{14}$,	$\frac{160}{39}$,		&c.

each of which fractions expresses the square root of 19 nearer than any preceding one, as is evident from art. 142; and it is manifest, that they may be continued at pleasure to any degree of accuracy required.

The operation in this partial example is obvious:

we first find the greatest integer contained in $\sqrt{19}$, which is 4, whence

$$\sqrt{19}=4+\frac{\sqrt{19}-4}{1};$$

and this quantity being transformed to the following form, by multiplying both numerator and denominator by $\sqrt{19}+4$, we have

$$\sqrt{19}=4+\frac{\sqrt{19}-4}{1}=4+\frac{3}{\sqrt{19}+4}=4+\frac{1}{\frac{\sqrt{19}+4}{3}}.$$

We then proceed to find the greatest integer contained in $\frac{\sqrt{19}+4}{3}$, which is 2; hence this fraction becomes

$$\frac{\sqrt{19}+4}{3}=2+\frac{\sqrt{19}-2}{3}=2+\frac{5}{\sqrt{19}+2}=2+\frac{1}{\frac{\sqrt{19}+2}{5}}.$$

And in the same manner we find the greatest integer contained in this last fraction, and so on, till we arrive at the fraction $\frac{\sqrt{19}-4}{1}$, which being the same as the first, all the terms will again recur in the same order, *ad infinitum*; and, consequently, the operation from that period may be discontinued. And it is obvious that the same principles may be applied to any quantity of the form

$$\frac{\sqrt{N}+M}{P}.$$

144. The above operation, which is tedious according to the method that has been explained, and which was necessary in order to show the origin of the rule, becomes extremely simple, by observing the

following law in the formation of the successive quotient; *viz.* let

$$\frac{\sqrt{19}+m}{n}=u+\ \&c.$$

$$\frac{\sqrt{19}+m'}{n'}=u'+\ \&c.$$

represent any two consecutive fractions in the foregoing example, u and u' being their respective quotients, then will

$$m'=nu-m,\ \text{and}$$

$$n'=\frac{19-m'^2}{n};$$

so that each value of m', n', and u', is deduced from those m, n, and u, in the preceding fraction: hence the foregoing operation, by means of this law, will stand thus:

$\frac{\sqrt{19}+0}{1}=4+\ \&c.$	$1\,.\,4-0=4;\ \frac{19-4^2}{1}=3.$
$\frac{\sqrt{19}+4}{3}=2+\ \&c.$	$3\,.\,2-4=2;\ \frac{19-2^2}{3}=5.$
$\frac{\sqrt{19}+2}{5}=1+\ \&c.$	$5\,.\,1-2=3;\ \frac{19-3^2}{5}=2.$
$\frac{\sqrt{19}+3}{2}=3+\ \&c.$	$2\,.\,3-3=3;\ \frac{19-3^2}{2}=5.$
$\frac{\sqrt{19}+3}{5}=1+\ \&c.$	$5\,.\,1-3=2;\ \frac{19-2^2}{5}=3.$
&c. &c.	

Where the calculations on the right hand of the line are set down only to explain the operation, but they are unnecessary when this is once under-

stood; and hence the extraction of the square root by this method becomes very simple.

145. This law has at present only been deduced from observation, but the universality of it may be demonstrated as follows:

Let

$$\frac{\sqrt{N}+m}{n}=u+\frac{\sqrt{N}+m-nu}{n}, \text{ and}$$

$$\frac{\sqrt{N}+m'}{n'}=u+\ \&c.$$

be any two consecutive fractions derived from the $\sqrt{N}$, N being any integer whatever not a complete square; then, from the nature of the operation, we must have

$$\frac{\sqrt{N}+m'}{n'}=\frac{n}{\sqrt{N}-(nu-m)}, \text{ or}$$

$$(\sqrt{N}+m')\times\{\sqrt{N}-(nu-m)\}=nn',$$

and since this product is an integer, n and n' being each whole numbers, it follows, that $m'=nu-m$, for otherwise the product of the two factors would not be rational; whence again

$$(\sqrt{N}+m')(\sqrt{N}-m')=N-m'^2=nn', \text{ or}$$

$$n'=\frac{N-m'^2}{n};$$

so that the law is universal.

And hence the square root of any number N, not a complete square, may be extracted in the following manner, supposing a to be the greatest integer contained in $\sqrt{N}$, and u, u', u'', &c., the greatest integers contained in the respective fractions to which they correspond; *viz.*

$$\frac{\sqrt{N}+0}{1} = a + \&c. \quad 1 \cdot a - 0 = m; \quad \frac{N - m^2}{1} = n.$$
$$\frac{\sqrt{N}+m}{n} = u + \&c. \quad n \cdot u - m = m'; \quad \frac{N - m'^2}{n} = n'.$$
$$\frac{\sqrt{N}+m'}{n'} = u' + \&c. \quad n' \cdot u' - m' = m''; \quad \frac{N - m''^2}{n'} = n''.$$
$$\frac{\sqrt{N}+m''}{n''} = u'' + \&c. \quad n'' \cdot u'' - m'' = m'''; \quad \frac{N - m'''^2}{n''} = n'''.$$
&c. &c.

And by continuing thus the extraction, we shall always arrive at a fraction equal to $\frac{\sqrt{N}+m}{n}$; after which, the quotients will recur again in the same order, *ad infinitum*, as will be demonstrated in the following propositions.

146. Thus the extraction of $\sqrt{23}$ (omitting the calculations on the right hand side of the line, which are supplied very readily as we proceed) becomes,

$$\frac{\sqrt{23}+0}{1} = 4 + \&c.$$
$$\frac{\sqrt{23}+4}{7} = 1 + \&c.$$
$$\frac{\sqrt{23}+3}{2} = 3 + \&c.$$
$$\frac{\sqrt{23}+3}{7} = 1 + \&c.$$
$$\frac{\sqrt{23}+4}{1} = 8 + \&c.$$
$$\frac{\sqrt{23}+4}{7} = 1 + \&c.$$

And having thus arrived at a fraction equal to

the second $\frac{\sqrt{23}+4}{7}$, the operation may be discontinued, as the quotients after this recur in the same order as at first; and hence we may calculate the series of fractions converging towards $\sqrt{23}$ to any degree of accuracy required; thus:

Quotients, 4; 1, 3, 1, 8; 1, 3, 1, 8; 1, &c.

Conv. frac. $\frac{4}{1}$, $\frac{5}{1}$, $\frac{19}{4}$, $\frac{24}{5}$, $\frac{211}{44}$, &c.

Scholium. Numbers falling under any of the following forms, *viz.*

$$p^2 \pm 1, \; p^2 \pm p, \text{ or } p^2 \pm \frac{2}{m}p,$$

have their square roots very readily extracted by continued fractions, the period of circulation never exceeding three terms: thus, for examples,

$$\frac{\sqrt{17}+0}{1} = 4 + \text{ \&c.}$$

$$\frac{\sqrt{17}+4}{1} = 8 + \text{ \&c.}$$

which last quotient will be repeated, *ad infinitum.*

$$\frac{\sqrt{15}+0}{1} = 3 + \text{ \&c.}$$

$$\frac{\sqrt{15}+3}{6} = 1 + \text{ \&c.}$$

$$\frac{\sqrt{15}+3}{1} = 6 + \text{ \&c.}$$

the two last of which quotients will be repeated as before.

And it is the same with all numbers falling under any of the above forms.

PROP. VI.

147. The series of quotients arising from the extraction of the square root of any number N, not a square, will be periodical.

We have already seen, that this has been the case in the partial examples which we have given in the foregoing proposition; and it is here proposed to demonstrate, that this law must necessarily have place for every possible value N, when it is not a square.

First, let us suppose $\frac{p^\circ}{q^\circ}$, $\frac{p}{q}$, $\frac{p'}{q'}$, to be any consecutive fractions, converging towards the $\sqrt{N}$; and let u°, u, u', be the corresponding quotients, u' being supposed the greatest integer contained in the complete quotient $\frac{\sqrt{N}+m}{n}$: so that, in the following expressions,

$$u^\circ,\ u,\ u',$$

$$\frac{p^\circ}{q^\circ},\ \frac{p}{q},\ \frac{p'}{q'},\ \text{\&c., we have}$$

$$\frac{p'}{q'}=\frac{up+p^\circ}{uq+q^\circ}.$$

And if instead of u we take the complete quotient $\frac{\sqrt{N}+m}{n}$, whence u was derived, we shall have, in the place of the foregoing equation,

$$\sqrt{N}=\frac{p\dfrac{\sqrt{N}+m}{n}+p^\circ}{q\dfrac{N+m}{n}+q^\circ}\ \text{(art. 139).}$$

which becomes, by reduction,

$$\sqrt{N}=\frac{p\sqrt{N}+pm+p^{\circ}n}{q\sqrt{N}+qm+q^{\circ}n};$$

whence we draw the equation

$$qN+\sqrt{N}(qm+q^{\circ}n)=p\sqrt{N}+pm+p^{\circ}n;$$

and since here we must have the rational part equal to the rational, and the irrational to the irrational, we obtain the two following equations:

$$qN=pm+p^{\circ}n,$$
$$p=qm+q^{\circ}n.$$

Multiply the first by q°, and the second by p°, gives

$$qq^{\circ}N=pq^{\circ}m+p^{\circ}q^{\circ}n,$$
$$pp^{\circ}=qp^{\circ}m+p^{\circ}q^{\circ}n;$$

then, by subtraction,

$$qq^{\circ}N-pp^{\circ}=(pq^{\circ}-qp^{\circ})m, \text{ and}$$
$$pp-Nqq=(pq^{\circ}-qp^{\circ})n;$$

this last being derived in a similar manner, by multiplying the first equations by q and p.

Now, by the property of continued fractions (art. 140), we have

$$pq^{\circ}-qp^{\circ}=+1, \text{ if } \frac{p}{q}>\sqrt{N};$$

$$pq^{\circ}-qp^{\circ}=-1, \text{ if } \frac{p}{q}<\sqrt{N}.$$

Whence it appears, that $pq^{\circ}-qp^{\circ}$ has always the same sign as $pp-Nqq$; because, if $\frac{p}{q}>\sqrt{N}$, $\frac{pp}{qq}>N$; and, consequently, $pp>Nqq$; and the contrary, if $\frac{p}{q}<\sqrt{N}$; and hence again it follows, that n is always

positive, because $pp - \text{N}qq = (pq^\circ - qp^\circ)n$, and $pp - \text{N}qq$, and $(pq^\circ - qp^\circ)$, have always the same sign. And this furnishes us with the means of ascertaining the limits of m and n; for, since

$$n' = \frac{\text{N} - m'^2}{n} \text{ (art. 145)},$$

and n and n' are positive, it is evident, that $m'^2 < \text{N}$, or $m' < \sqrt{\text{N}}$; also, m' being an integer, it can never exceed the greatest integer contained in $\sqrt{\text{N}}$. And since $m = nu - m'$ (by the same article), or $m + m' = nu$, and m and m' are each $< \sqrt{\text{N}}$, it follows, that neither n, nor u, nor nu, can be greater than $m + m'$; and we have seen, that neither m nor m' can exceed a (supposing a to be the greatest integer contained in $\sqrt{\text{N}}$), therefore, neither n nor u can exceed $2a$; or, which is the same, $2a$ is the limit both of m and the quotient u.

And hence it appears, that in the transformation of $\sqrt{\text{N}}$ into continued or converging fractions, which (from art. 145) has always the form

$$\begin{array}{l}
\dfrac{\sqrt{\text{N}} + 0}{1} = a + \&c. \\
\dfrac{\sqrt{\text{N}} + m}{n} = u + \&c. \\
\dfrac{\sqrt{\text{N}} + m'}{n'} = u' + \&c. \\
\dfrac{\sqrt{\text{N}} + m''}{n''} = u'' + \&c. \\
\quad \&c. \qquad\quad \&c.
\end{array}$$

since m, n, and u, can never exceed certain limits; that is, m not $> a$, n not $> 2a$, and u not $> 2a$:

also, the expression itself being infinite, the same values of m and n must necessarily come together an infinite number of times; and thus form a series of periodical quotients, which will continue to be repeated *ad infinitum*, as we have seen in the partial examples in art. 143. — Q. E. D.

PROP. VII.

148. In any series of quotients derived from $\sqrt{N}$, the second is that which first recurs, and commences the second, and all the other periods of circulation; that is, the quotients always recur in the same order as at first, excepting only the first a, which expresses the greatest integer contained in $\sqrt{N}$.

In order to demonstrate this (since we know that the quotients recur in periods), we shall suppose the first period to be

$$\begin{array}{l} a;\ \alpha,\ \beta,\ \gamma,\ \delta,\ \&c.\ -\ -\ -\ \lambda,\ u,\ u',\ u'',\ \&c.;\ \text{and} \\ -\ -\ -\ -\ -\ -\ -\ -\ w,\ u,\ u',\ u'',\ \&c., \end{array}$$

part of the second period; and then prove, that $\lambda = w$, the quotient preceding λ = that preceding w, and so on to α; which must, therefore, necessarily be that quotient which commences each of the periods.

Let, then,

$$\left\{\begin{array}{l} a;\ \alpha,\ \beta,\ \gamma,\ -\ -\ -\ \lambda,\ u,\ u',\ u'',\ \&c.\ w,\ u,\ u',\ u''; \\ \dfrac{a}{1},\ \&c.\ -\ -\ -\ \dfrac{p^\circ}{q^\circ},\ \dfrac{p}{q},\ \ -\ -\ -\ \ \dfrac{P^\circ}{Q^\circ},\ \dfrac{P}{Q}; \end{array}\right.$$

represent any series of quotients, and their corresponding converging fractions; also, let

$$\frac{\sqrt{N}+a}{b} \; - \; - \; - \; \frac{\sqrt{N}+m^\circ}{n^\circ}, \quad \frac{\sqrt{N}+m}{n};$$

$$- \; - \; - \; - \; - \; \frac{\sqrt{N}+\mathrm{m}}{\mathrm{n}}, \quad \frac{\sqrt{N}+m}{n},$$

be the corresponding complete quotients.

Then, from what has been demonstrated (art. 145), we have $N - m^2 = nn^\circ$, and $N - m^2 = n\mathrm{n}$; whence $n^\circ = \mathrm{n}$; and we shall also have (by the same article) $m = \lambda n^\circ - m^\circ$, and $m = w\mathrm{n} - \mathrm{m}$;

whence we draw $\dfrac{m^\circ - \mathrm{m}}{n^\circ} = \lambda - w$. But (art. 147) $qm + q^\circ n = p$, or $m = \dfrac{p}{q} - \dfrac{q^\circ n}{q}$; and since $\dfrac{p}{q}$ is an approximate value of $\sqrt{N}$, we must have $\dfrac{p}{q} = a +$ a fraction $\dfrac{r}{q}$ (a being as above the greatest integer in $\sqrt{N}$), and hence result

$$a - m = \frac{q^\circ n - r}{q}.$$

And since $q^\circ < q$, from the nature of continued fractions, we shall have $a - m < n$; and in the same manner $a - m^\circ < n^\circ$, $a - \mathrm{m} < \mathrm{n}$; and, therefore, *a fortiori*, $m^\circ - \mathrm{m} < n^\circ$. But we have found $\dfrac{m^\circ - \mathrm{m}}{n^\circ} = \lambda - w$, which must necessarily be an integer or zero, because λ and w are each whole numbers; and since $m^\circ - \mathrm{m} < n^\circ$, this cannot be an integer; it must, therefore, be zero, that is, $m^\circ = \mathrm{m}$, or $\lambda = w$. And, in the same manner, it may be proved, that the quotient preceding w is the same as that

preceding λ, and so on till we arrive at the quotient α; and, consequently, it is this which first recurs, and commences every period. — Q. E. D.

PROP. VIII.

149. The last quotient of every complete period of quotients is equal to $2a$, a being the greatest integer contained in $\sqrt{N}$.

Since we know the period of circulation by the foregoing proposition, we may now represent the series of quotients, converging towards $\sqrt{N}$, and their corresponding converging fractions, as follows; *viz.*

$$a;\ \alpha,\ \beta,\ \gamma,\ \delta,\ -\ \ -\ \lambda,\ u;\ \alpha,\ \beta,\ \gamma,\ -\ -\ -\ \lambda,\ u;\ \&c.$$
$$\frac{a}{1},\ -\ -\ -\ -\ \frac{p^\circ}{q^\circ},\ \frac{p}{q},\ \frac{p'}{q'},\ -\ -\ -\ \frac{P^\circ}{Q^\circ},\ \frac{P}{Q},\ \&c.$$

so that $\frac{p}{q}$ is the converging fraction, which corresponds to the last quotient u, of the first period

$\alpha,\ \beta,\ \gamma,\ \delta,$ &c. $\lambda,\ u$; and let

$$\frac{\sqrt{N}+m}{n}$$

be the complete quotient whence u is derived; that is,

$$\frac{\sqrt{N}+m}{n} = u + \ \&c.$$

then, on the same principles as in art. 147,

$$\sqrt{N} = \frac{p\dfrac{\sqrt{N}+m}{n} + p^\circ}{q\dfrac{\sqrt{N}+m}{n} + q^\circ}.$$

Now, if we attend to the law of formation, we shall have,

$$\frac{\sqrt{N}+a}{N-a^2},$$

for the complete quotient, answering to $\frac{a}{1}$, which will be equal to that succeeding

$$\frac{\sqrt{N}+m}{n}.$$

But it is obvious, from art. 145, that

$$\frac{\sqrt{N}+m}{n}=u+\frac{\sqrt{N}-(nu-m)}{n};$$

and the succeeding complete quotient is

$$\frac{\sqrt{N}+(nu-m)}{\frac{N-(nu-m)^2}{n}}=\frac{\sqrt{N}+a}{N-a^2},$$

whence $nu-m=a$, and, consequently, we have

$$\frac{\sqrt{N}+m}{n}=u+\frac{\sqrt{N}-a}{n}.$$

It also follows, from the above, that

$$\frac{N-(nu-m)^2}{n}=\frac{N-a^2}{n}=N-a^2,$$

whence we have $n=1$; and, therefore,

$$\frac{\sqrt{N}+m}{n}=w+\frac{\sqrt{N}-a}{n}, \text{ becomes}$$

$$\frac{\sqrt{N}+m}{n}=u+\sqrt{N}-a;$$

and, substituting this value of $\frac{\sqrt{N}+m}{n}$ in the original expression for $\sqrt{N}$, *viz.*

$$\sqrt{N} = \frac{p\dfrac{\sqrt{N}+m}{n} + p^\circ}{q\dfrac{\sqrt{N}+m}{n} + p^\circ},$$

we deduce immediately this equation,

$$\sqrt{N} = \frac{p\sqrt{N} + p(u-a) + p^\circ}{q\sqrt{N} + q(u-a) + q^\circ},$$

which furnishes the two following equations;

$$p(u-a) + p^\circ = Nq,$$
$$q(u-a) + q^\circ = p,$$

the second of which gives by division

$$(u-a) + \frac{q^\circ}{q} = \frac{p}{q};$$

whence again it follows, that $u-a$ is the greatest integer contained in $\frac{p}{q}$; but as this fraction is an approximation towards $\sqrt{N}$, the greatest integer contained in it is a: we have, therefore, $u-a=a$, or $u=2a$; that is, the last quotient in the period $=2a$.—Q. E. D.

PROP. IX.

150. The equation $p^2 - Nq^2 = 1$ is always possible in integers, if N be any integer number whatever not a square.

For, by the foregoing proposition, the complete quotient answering to the last quotient in any period, as $\frac{\sqrt{N}+m}{n} = u +$ &c., is such, that $u=2a$ (a being the greatest integer contained in $\sqrt{N}$); and, consequently, as we have seen, $n=1$, because

$2a$ is the limit of nu (art. 147), therefore $m = 2a$. If, now, we represent by $\frac{p^\circ}{q^\circ}$, and $\frac{p}{q}$, two converging fractions, the latter corresponding to the quotient $2a$, we have also (by art. 147)

$$p^2 - \text{N}q^2 = (pq^\circ - p^\circ q)n;$$

but, in the present case, $n = 1$, and $pq^\circ - p^\circ q = \pm 1$, by the property of continued fractions; therefore,

$$p^2 - \text{N}q^2 = \pm 1;$$

the upper sign having place when $\frac{p}{q} > \sqrt{\text{N}}$, and the lower one when $\frac{p}{q} < \sqrt{\text{N}}$.

But all the converging fractions in the even places are $> \sqrt{\text{N}}$, and all those in the odd places $< \sqrt{\text{N}}$, as is evident, because they are alternately greater and less than $\sqrt{\text{N}}$, and the first is always less than $\sqrt{\text{N}}$; but since these periods of quotients recur *ad infinitum*, if $\frac{p}{q}$, the first fraction answering to the quotient $2a$, be not in an even place, it must necessarily be so when that quotient recurs again; and, consequently, the equation

$$p^2 - \text{N}q^2 = 1$$

is always possible, N being any integer number not a square; and there are an infinite number of values, that may be given to p and q, which answer the conditions of the equation; *viz.* every fraction $\frac{p}{q}$ standing in an even place, and corresponding to the quotient $2a$.—Q. E. D.

Cor. 1. It appears, from the foregoing proposition, that the equation

$$p^2 - \text{N}q^2 = -1$$

is also possible in all cases where the quotient $2a$ occurs first in an odd place, and that there are likewise an infinite number of values that may be given to p and q, which will answer the required conditions; but if $2a$ occur first in an even place, then the equation

$$p^2 - \text{N}q^2 = -1$$

is impossible.

Cor. 2. Hence also the indeterminate equation

$$x^2 - ay^2 = z^2$$

is always possible in integers; for the equation

$$x^2 - ay^2 = 1, \text{ gives}$$
$$x^2z^2 - ay^2z^2 = z^2:$$

this equation, therefore, is always solvible in integers; which has in fact been otherwise demonstrated in Part I.

151. It will not be amiss to illustrate what has been demonstrated in the foregoing propositions by a few examples:

Ex. 1. Find the values of x and y in the equation

$$x^2 - 15y^2 = 1.$$

Here we have, by the conversion of $\sqrt{15}$,

$\frac{\sqrt{15}+0}{1} = 3 + \&c.$	$1 . 3 - 0 = 3;\ \frac{15-3^2}{1} = 6.$
$\frac{\sqrt{15}+3}{6} = 1 + \&c.$	$6 . 1 - 3 = 3;\ \frac{15-3^2}{6} = 1.$
$\frac{\sqrt{15}+3}{1} = 6 + \&c.$	$1 . 6 - 3 = 3;$ &c.

Quotients, 3, 1, 6, 1, 6, &c.

Fractions, $\frac{3}{1}$, $\frac{4}{1}$, &c.

Now the first fraction $\frac{4}{1}$, which answers to the quotient $2a$, is in an even place; we have, therefore, $x=4$, and $y=1$, which gives

$$4^2-15.1^2=1.$$

Ex. 2. Find the values of x and y in the equation

$$x^2-17y^2=1.$$

First,

$$\frac{\sqrt{17}+0}{1}=4+\&c. \quad \Big| \quad 1.4-0=4; \quad \frac{\sqrt{17}-4^2}{1}=1.$$

$$\frac{\sqrt{17}+4}{1}=8+\&c. \quad \Big| \quad 1.8-4=4; \quad \frac{\sqrt{17}-4^2}{1}=1.$$

$$\frac{\sqrt{17}+4}{1}=8+\&c. \quad \Big| \quad 1.8-4=4; \quad \&c.$$

Quotients, 4, 8, 8, 8, 8, &c.

Fractions, $\frac{4}{1}$, $\frac{33}{8}$.

And here, the first fraction corresponding to 8 being in an odd place, we employ the second, which gives $x=33$ and $y=8$, whence

$$33^2-17.8^2=1.$$

Ex. 3. Find the values of x and y in the equation

$$x^2 - 13y^2 = 1.$$

First,

$$\begin{array}{l|l}
\dfrac{\sqrt{13}+0}{1} = 3 + \&c. & 1.3 - 0 = 3; \quad \dfrac{13 - 3^2}{1} = 4. \\
\dfrac{\sqrt{13}+3}{4} = 1 + \&c. & 4.1 - 3 = 1; \quad \dfrac{13 - 1^2}{4} = 3. \\
\dfrac{\sqrt{13}+1}{3} = 1 + \&c. & 3.1 - 1 = 2; \quad \dfrac{13 - 2^2}{3} = 3. \\
\dfrac{\sqrt{13}+2}{3} = 1 + \&c. & 3.1 - 2 = 1; \quad \dfrac{13 - 1^2}{3} = 4. \\
\dfrac{\sqrt{13}+1}{4} = 1 + \&c. & 4.1 - 1 = 3; \quad \dfrac{13 - 3^2}{4} = 1. \\
\dfrac{\sqrt{13}+3}{1} = 6 + \&c. & 1.6 - 3 = 3; \quad \&c.
\end{array}$$

which last gives the quotient $2a$, or 2.3; we have, therefore, for

Quotients, 3, 1, 1, 1, 1, 6; 1, 1, 1, 1, 6; 1, &c.

Fractions, $\frac{3}{1}, \frac{4}{1}, \frac{7}{2}, \frac{11}{3}, \frac{18}{5}, \frac{119}{33}, \frac{137}{38}, \frac{256}{71}, \frac{393}{109}, \frac{649}{180}.$

Now here again the first fraction answering to the quotient 6, being in an odd place, we proceed till we meet with 6 a second time, which will necessarily be in an even place; and the fraction corresponding to it is $\frac{649}{180}$, so that $x = 649$ and $y = 180$ are the least values of x and y, that answer the conditions of the equation

$$x^2 - 13y^2 = 1.$$

If the proposed equation had been

$$x^2 - 13y^2 = -1,$$

we should have had, $x=18$ and $y=5$, for the least values of x and y that satisfy this equation.

But if the first fraction answering to the quotient $2a$ be not found in an odd place when it first occurs, then it follows, from what has been demonstrated, that the equation

$$x^2-Ny^2=-1$$

is impossible, as we have before observed.

152. *Scholium.* The solution of the equation

$$x^2-Ny^2=1$$

is one of the most important problems in the indeterminate analysis, it being necessary to the solution of many other interesting questions of this kind; and, notwithstanding the method we have given is direct and simple, yet the least values of x and y in many cases being very great, the task of finding them is very laborious: thus the least values of x and y that solve the equation

$$x^2-211y^2=1, \text{ are}$$

$$x=278354373650, \text{ and } y=19162705353.$$

And the equation

$$x^2-5658y^2=1$$

has the least values of x and y as follows; *viz.*

$$x=\begin{cases}166100725257977318398207998462201 32\\ \quad 4702014613503.\end{cases}$$

$$y=\begin{cases}698253616416770487157775940222021 00\\ \quad 2391003072.\end{cases}$$

These circumstances have induced a few celebrated mathematicians to form tables of the values of x and y, necessary for the solution of the equation $x^2-Ny^2=1$.

Euler first undertook this task, for all values of N from 1 to 100, which was afterwards doubled by Lagrange, both of which tables are given in the second volume of Euler's Algebra. But Legendre has extended the same to upwards of 1000, at least for the solution of the equation

$$x^2 - Ny^2 = \pm 1;$$

and he has shown the method of deducing from them the solution of every possible equation

$$x^2 - Ny^2 = + A,$$

whether the numbers in his table give

$$x^2 - Ny^2 = -1, \text{ or } x^2 - Ny^2 = -1:$$

a part of this table is subjoined to the present work, which will be found useful in many cases.— See Table II.

PROP. X.

153. Given the difference between $\frac{p}{q}$ and $\sqrt{N}$; *viz.*

$$\frac{p}{q} - \sqrt{N} = \frac{\delta}{q^2},$$

δ being less than unity, to find the necessary conditions for the value of δ, that $\frac{p}{q}$ may be a fraction arising from the extraction of $\sqrt{N}$.

Let the given fraction $\frac{p}{q}$ be converted into a series of converging fractions, giving the

Quotients, $a,\ b,\ c,\ \text{- - -}\ u.$

Conv. frac. $\frac{a}{1},\ \frac{ab+1}{b}\ \text{- - -}\ \frac{p^\circ}{q^\circ},\ \frac{p}{q}.$

Now if $\frac{p}{q}$ be a fraction converging towards $\sqrt{N}$, it follows, that all the quotients a, b, c, &c. are likewise obtained from the same development; and, consequently, that the quotient u is followed by others, u', u'', u''', &c. Let now the complete quotient, answering to the fraction $\frac{p}{q}$, be

$$\frac{\sqrt{N}+m}{n},$$

then we have, on the same principles as in art. 147,

$$\sqrt{N}=\frac{p\frac{\sqrt{N}+m}{n}+p^{\circ}}{q\frac{\sqrt{N}+m}{n}+q^{\circ}}.$$

Or, by substituting for the complete quotient

$$\frac{\sqrt{N}+m}{n}=\mu,$$

the above expression will become

$$\sqrt{N}=\frac{p\mu+p^{\circ}}{q\mu+q^{\circ}}.$$

Whence, by substituting for $\sqrt{N}$, we have

$$\sqrt{N}-\frac{p}{q}=\frac{p^{\circ}q-pq^{\circ}}{q(q\mu+q^{\circ})}=\frac{1}{q(q\mu+q^{\circ})};$$

which last expression must be equal to $\frac{\delta}{q^2}$; that is,

$$\frac{\delta}{q^2}=\frac{q}{q^2(q\mu+q^{\circ})}; \text{ or } \delta=\frac{q}{q\mu+q^{\circ}}.$$

Now since μ is the complete quotient corre-

sponding with the fraction $\frac{p}{q}$, it must be positive, and greater than unity, and, therefore, $\delta < \frac{q}{q+q^\circ}$; and hence, conversely, if $\frac{q}{q+q^\circ} > \delta$, the value of μ must necessarily be positive, and greater than unity; and, consequently, $\frac{p}{q}$ will, in this case, be a fraction converging towards $\sqrt{N}$.

That is, if $\frac{p}{q}$ be any fraction, and the difference

$$\frac{p}{q} - \sqrt{N} = \frac{\delta}{q^2}, \text{ and } \delta < \frac{q}{q+q^\circ};$$

then is $\frac{p}{q}$ a fraction, which arises in the development of $\sqrt{N}$ into converging fractions. Which is the condition required to be found.

PROP. XI.

154. If the indeterminate equation

$$x^2 - Ny^2 = \pm A,$$

be possible (A being $< \sqrt{N}$), A must be found in the denominator of one of the complete quotients, arising from the development of $\sqrt{N}$.

It appears from art. 147, that when A is found in the denominator of any complete quotient, as

$$\frac{\sqrt{N}+m}{n};$$

that is, when $n = A$, and $\frac{p^\circ}{q^\circ}$, $\frac{p'}{q'}$, be two converg-

ing fractions, the latter corresponding with this complete quotient, we shall have

$$p^2 - Nq^2 = A(pq^\circ - p^\circ q); \text{ or, since}$$
$$pq^\circ - p^\circ q = \pm 1, \text{ we obtain}$$
$$p^2 - Nq^2 = \pm A.$$

And it is here proposed to demonstrate, that this equation can only have place when A is thus found in the denominator of one of the complete quotients, derived from $\sqrt{N}$, A being always supposed less than $\sqrt{N}$.

Now, first, from the equation

$$p^2 - Nq^2 = \pm A, \text{ we obtain}$$

$$p - q\sqrt{N} = \frac{\pm A}{p + q\sqrt{N}}; \text{ or}$$

$$\frac{p}{q} - \sqrt{N} = \frac{\pm A}{q(p + q\sqrt{N})}.$$

And, if we represent, as in the foregoing article,

$$\frac{p}{q} - \sqrt{N} \text{ by } \frac{\delta}{q^2}, \text{ we have}$$

$$\frac{\delta}{q^2} = \frac{\pm A}{q(p + q\sqrt{N})}, \text{ or } \delta = \frac{\pm Aq}{p + q\sqrt{N}}.$$

Let now $\frac{p^\circ}{q^\circ}$ be the converging fraction preceding $\frac{p}{q}$, in the series of fractions arising from the development of $\frac{p}{q}$; then, by the preceding article, we have to prove that

$$\frac{\text{A}q}{p+q\sqrt{\text{N}}} < \frac{q}{q+q^{\circ}};$$

for in that case it necessarily follows, that $\frac{p}{q}$ is a fraction arising from the development of $\sqrt{\text{N}}$ (art. 153).

Now, since $\frac{p}{q} - \sqrt{\text{N}} = \frac{\delta}{q^2}$, we have

$$p = q\sqrt{\text{N}} + \frac{\delta}{q}; \text{ again, if}$$

$$\frac{\text{A}q}{p+q\sqrt{\text{N}}} < \frac{q}{q+q^{\circ}}, \text{ so is also}$$

$$\text{A}(q+q^{\circ}) < (p+q\sqrt{\text{N}});$$

or, substituting for p, it becomes

$$\text{A}(q+q^{\circ}) < (2q\sqrt{\text{N}} + \frac{\delta}{q}).$$

Now this inequality is readily demonstrated; for it may be put under the form

$$2q\sqrt{\text{N}} - \text{A}(q+q^{\circ}) + \frac{\delta}{q} > 0,$$

$$(q+q^{\circ})(\sqrt{\text{N}} - \text{A}) + (q-q^{\circ})\sqrt{\text{N}} + \frac{\delta}{q} > 0;$$

and since $\sqrt{\text{N}} > \text{A}$, and $q > q^{\circ}$, the whole of this expression is positive; and, therefore, > 0, at least when δ is positive; and if δ were negative, we should have evidently

$$(q-q^{\circ})\sqrt{\text{N}} > \frac{\delta}{q};$$

and, therefore, in either case the inequality is established; that is,

$$\frac{Aq}{p+q\sqrt{N}} < \frac{q}{q+q^{\circ}};$$

and, consequently, $\frac{p}{q}$ is found among the fractions converging towards the $\sqrt{N}$.

Therefore, when it is required to find the values of x and y in the equation

$$x^2 - Ny^2 = \pm A;$$

A being $< \sqrt{N}$, we must convert N into a continued fraction, by the forms given in art. 145; and if A be found in the denominator of any one of the complete quotients obtained by this development, we shall have the solution sought, by finding the converging fraction answering to this quotient, which solution will give

$$x^2 - Ny^2 = A, \text{ or } x^2 - Ny^2 = -A,$$

according as the fraction is found in an even or odd place; and if A be not found in an odd place, the latter equation is impossible; and if A be not found in the denominator of any of these complete quotients, we may be assured, that the proposed equation is impossible under either sign.

Ex. 1. Find the values of x and y in the equation

$$x^2 - 23y^2 = 2.$$

First, by the development of $\sqrt{23}$, we have

$$\frac{\sqrt{23}+0}{1} = 4 + \&c.$$

$$\frac{\sqrt{23}+4}{7} = 1 + \&c.$$

$$\frac{\sqrt{23}+3}{2} = 3 + \&c.$$

and in this last fraction, 2 being found in the denominator, we have

$$\text{Quotients,} \quad 4, \ 1, \ 3, \ \&c.$$

$$\text{Fractions,} \quad \frac{4}{1}, \ \frac{5}{1}, \ \&c.$$

the last of which, answering to the quotient 3, gives $x=5$, and $y=1$; so that

$$x^2-23y^2=2,$$

as was required.

Ex. 2. Required the possibility or impossibility of the equations

$$\begin{cases} x^2-17y^2= & 3, \\ x^2-17y^2= & 2, \\ x^2-17y^2= & -3, \\ x^2-17y^2= & -2. \end{cases}$$

First, by the development of $\sqrt{17}$, we have

$$\frac{\sqrt{17}+0}{1}=4+\ \&c.$$

$$\frac{\sqrt{17}+4}{1}=8+\ \&c.$$

$$\&c. \qquad\qquad \&c.$$

whence it follows, that since neither 2 nor 3 enters into the denominator of the complete quotients, the equations are all impossible.

Cor. 1. The indeterminate equation

$$x^2-(a^2+1)y^2=\pm\text{A}$$

is always impossible, if $\text{A}>1$ and $<\sqrt{(a^2+1)}$; because the complete quotients arising from $\sqrt{(a^2+1)}$ have only unity enter for a denominator: we must of course except those cases also in which A is a

complete square, as these will always be possible from the equation $x^2 - \text{N}y^2 = 1$.

For, by the forms art. 145, we have

$$\frac{\sqrt{(a^2+1)}+0}{1} = a + \text{ \&c.}$$

$$\frac{\sqrt{(a^2+1)}+a}{1} = 2a + \text{ \&c.}$$

which last complete quotient will be repeated to infinity.

Cor. 2. The indeterminate equation

$$x^2 - (a^2-1)y^2 = \pm \text{A}$$

is also impossible, under the same limitations, because, by art. 145, we have

$$\frac{\sqrt{(a^2-1)}+0}{1} = (a-1) + \text{ \&c.}$$

$$\frac{\sqrt{(a^2-1)}+(a-1)}{2a-2} = 1 + \text{ \&c.}$$

$$\frac{\sqrt{(a^2-1)}+(a-1)}{1} = 2(a-1) + \text{ \&c.}$$

and these two last complete quotients will be repeated *ad infinitum;* and, consequently, only 1 and $2(a-1)$ will ever be found in the denominators of them.

Cor. 3. The indeterminate equation

$$x^2 - (a^2+a)y^2 = \pm \text{A}$$

is always impossible, if $\text{A} > 1$ and $< a$, excepting, as before, those cases in which A is a complete square.

For

$$\frac{\sqrt{(a^2+a)}+0}{1} = a + \text{ \&c.}$$

$$\frac{\sqrt{(a^2+a)}+a}{a} = 2 + \text{\&c.}$$

$$\frac{\sqrt{(a^2+a)}+a}{1} = 2a + \text{\&c.}$$

The two last of which fractions will continually recur; and, consequently, the equation is always impossible under the above limitations.

Cor. 4. The indeterminate equation

$$x^2 - (a^2 - a)y^2 = \pm \text{A}$$

is always impossible, if A > 1 and $< (a-1)$, except the cases in which A is a complete square.

For

$$\frac{\sqrt{(a^2-a)}+0}{1} = (a-1) + \text{\&c.}$$

$$\frac{\sqrt{(a^2-a)}+(a-1)}{a-1} = 2 \qquad + \text{\&c.}$$

$$\frac{\sqrt{(a^2-a)}+(a-1)}{1} = 2(a-1) + \text{\&c.}$$

which two last quotients will be repeated, as before, *ad infinitum*; and, therefore, no number under the above limitations, will enter into their denominators; and, consequently, the equation is impossible.

PROP. XII.

155. If a be a prime number of the form $4n+1$, the equation

$$x^2 - ay^2 = -1$$

is always resolvible in integers.

Let p and q be least values (except 1 and 0) that satisfy the equation

$$p^2 - aq^2 = 1, \text{ or } p^2 - (4n+1)q^2 = 1;$$

then it is obvious that q must be even, for if it was odd, q^2 would be of the form $8n+1$, and

$$aq^2 + 1 \doteq (4n+1) \times (8n'+1) + 1 \doteq 4n'' + 2,$$

which cannot be a square: since, then, q must be even, let us make $q = 2mn$, m and n being integers prime to each other; then we shall have $p^2 - 1 = 4m^2n^2$; but p being odd, and, consequently, $p^2 - 1 \doteq 8n'$, it follows, that either m or n is even, and the other odd, for otherwise we should not have $p^2 - 1 \doteq 8n'$, and they cannot be both even, because they are prime to each other. Let us therefore suppose n to be odd, then the equation

$$(p+1)(p-1) = 4am^2n^2,$$

in which the factors $p+1$, and $p-1$, can have only the common measure 2 (and this must necessarily have place, because p is odd), will be resolvible into the four following forms:

$$1. \begin{cases} p+1 = 2am^2, \\ p-1 = 2n^2. \end{cases} \qquad 2. \begin{cases} p+1 = 2m^2, \\ p-1 = 2an^2. \end{cases}$$

$$3. \begin{cases} p+1 = 2an^2, \\ p-1 = 2m^2. \end{cases} \qquad 4. \begin{cases} p+1 = 2n^2, \\ p-1 = 2am^2. \end{cases}$$

Now the second and fourth of these forms give

$$1 = m^2 - an^2, \text{ or } 1 = n^2 - am^2;$$

which equations cannot have place, because m and n are less than p and q; and these last were the least that satisfied the equation $p^2 - aq^2 = 1$. There remain, therefore, only the first and the third, which give

$$n^2 - am^2 = -1, \text{ or } m^2 - an^2 = -1,$$

and one of these equations must necessarily obtain; but either of them resolves the equation

$$x^2 - ay^2 = -1,$$

which is, therefore, always possible, when a is a prime number of the form $4n+1$. It may also be observed, that, of the above two equations, the last is the only one that can obtain; for, since n is odd and m even, it is evident that the first cannot become equal to -1.

Cor. It results from this theorem, that when a is a prime number of the form $4n+1$, every number $\text{N} = \pm x^2 - ay^2$ is also $\pm ax'^2 - y'^2$; for since, in this case, we may suppose $m^2 - an^2 = -1$, we shall have

$$\text{N} = (x^2 - ay^2)(m^2 - an^2) = a(my + nx)^2 - (mx + any)^2.$$

PROP. XIII.

156. If a be a prime number of the form $8n+3$, the equation

$$x^2 - ay^2 = -2$$

is always resolvible in integers.

For let p and q be the least numbers that satisfy the equation

$$p^2 - aq^2 = 1;$$

then it is obvious, that p and q cannot be both even nor both odd: we must, therefore, have either p even and q odd, or q even and p odd; which divides this proposition into two distinct cases.

Case 1. *When* p *is even and* q *odd.*

Here, if we make $q = mn$, these quantities, m and

n, being supposed prime to each other, and both odd numbers, the equation

$$p^2 - 1 = aq^2$$

can only be resolved into factors in two different ways; *viz.*

$$1. \begin{cases} p+1 = am^2, \\ p-1 = n^2. \end{cases} \qquad 2. \begin{cases} p+1 = m^2, \\ p-1 = an^2. \end{cases}$$

The second of which forms gives $m^2 - an^2 = 2$, which cannot obtain; for m and n being both odd, and

$$a \doteq 8n' + 3, \text{ we have } an^2 + 2 = m^2, \text{ or}$$
$$m^2 \doteq (8n' + 3)(8n'' + 1) + 2 \doteq 8n''' + 2,$$

which is impossible. Therefore, if either of these forms be possible, it must be the first, which, by subtraction, becomes $n^2 - am^2 = -2$; in which case the equation $x^2 - ay^2 = -2$ will be possible.

Case 2. *When* q *is even and* p *odd.*

Here we may make $q = 2mn$; whence

$$p^2 - 1 = 4am^2n^2;$$

but since p is odd, $p^2 \doteq 8n' + 1$; and, consequently,

$$4m^2n^2 \doteq 8n';$$

therefore, either n or m is even, and the other odd: let, then, n be odd, and the equation

$$(p+1)(p-1) = 4am^2n^2,$$

in which the factors $(p+1)$ and $(p-1)$ must necessarily have a common measure 2 (and they can have no other), is resolvible into the four following forms; *viz.*

$$1. \begin{cases} p+1 = 2am^2, \\ p-1 = 2n^2. \end{cases} \qquad 2. \begin{cases} p+1 = 2m^2, \\ p-1 = 2an^2. \end{cases}$$

$$3. \begin{cases} p+1 = 2an^2, \\ p-1 = 2m^2. \end{cases} \qquad 4. \begin{cases} p+1 = 2n^2, \\ p-1 = 2am^2. \end{cases}$$

The first form gives $n^2 - am^2 = -1$, which is impossible; for, since n is odd and m even,

$$n^2 \doteq 4n' + 1, \text{ and } am^2 \doteq 4n'';$$

and, consequently, their difference cannot be equal to -1.

The second form gives $m^2 - an^2 = 1$; and thus p and q would not be the least numbers, that satisfy the equation

$$p^2 - aq^2 = 1;$$

which is contrary to the hypothesis.

The third form gives $m^2 - an^2 = -1$, which is also an impossible equation; for m being even, we should have

$$4n - (8n' + 3)(8n'' + 1) \doteq 4n''' + 1,$$

which can never become equal to -1.

The fourth form gives the same result as the second, and, therefore, cannot obtain for the same reason.

Hence it appears, that, of the several forms which have been given to the equation

$$p^2 - aq^2 = 1,$$

only one of them can be possible, and this is the equation

$$n^2 - am^2 = -2;$$

which arises in our first case, where we suppose $q = mn$: this, therefore, must necessarily obtain; that is, the equation

$$x^2 - ay^2 = -2$$

is always possible in integers, if a be a prime number of the form $8n + 3$.

PROP. XIV.

157. If a be a prime number of the form $8n-1$, the equation

$$x^2 - ay^2 = 2$$

is always resolvible in integers.

For let p and q be the least numbers that establish the equation

$$p^2 - aq^2 = 1,$$

then we may have either $q = mn$, or $q = 2mn$, according as we suppose q to be odd or even, which give the four following resolutions of the equation

$$p^2 - 1 = aq^2; \; viz.$$

$$1.\begin{cases} p+1 = am^2, \\ p-1 = n^2. \end{cases} \qquad 2.\begin{cases} p+1 = m^2, \\ p-1 = an^2. \end{cases}$$

$$3.\begin{cases} p+1 = 2am^2, \\ p-1 = 2n^2. \end{cases} \qquad 4.\begin{cases} p+1 = 2m^2, \\ p-1 = 2an^2. \end{cases}$$

The first of which forms gives

$$am^2 - n^2 = 2,$$

an equation that cannot obtain, because, m and n being both odd, the first side is of the form

$$(8n-1)(8n'+1) - (8n''+1) \doteq 8n''' - 2,$$

which can never be equal to 2.

The third form gives $am^2 - n^2 = 1$, which is also impossible; for if m and n were both odd, then $am^2 - n^2$ would be even, and, therefore, not equal to 1. If m was even and n odd, then

$$am^2 - n^2 \doteq 4n' + 3,$$

which cannot be equal to 1; and we have the same result by taking n even and m odd: therefore, this equation is impossible.

The fourth form gives $m^2 - an^2 = 1$, which cannot have place; because p and q are the least numbers that satisfy the equation $p^2 - aq^2 = 1$.

Therefore, the second is the only possible form, and this gives

$$m^2 - an^2 = 2\,;$$

and, consequently, the proposed equation

$$x^2 - ay^2 = 2$$

is always possible, when a is a prime of the form $8n - 1$.

158. Cor. If, in the equation $p^2 - aq^2 = 1$, we resolve a into any two factors prime to each other, as mn, we have, by transposition,

$$p^2 - 1 = mnq^2,$$

which equation may be decomposed into factors four different ways; *viz.*

$$1.\ \begin{cases} p + 1 = fmg^2, \\ p - 1 = fnh^2. \end{cases} \qquad 2.\ \begin{cases} p + 1 = fng^2, \\ p - 1 = fmh^2. \end{cases}$$

$$3.\ \begin{cases} p + 1 = fmng^2, \\ p - 1 = fh^2. \end{cases} \qquad 4.\ \begin{cases} p + 1 = fg^2, \\ p - 1 = fmnh^2. \end{cases}$$

From which result the four following equations:

$$\frac{2}{f} = mg^2 - nh^2, \quad \frac{2}{f} = ng^2 - mh^2,$$

$$\frac{2}{f} = mng^2 - h^2, \quad \frac{2}{f}g^2 = -mnh^2,$$

where f must be either 1 or 2, which numbers, being successively substituted for f, give the following eight combinations; *viz.*

$$\begin{matrix} 1. \\ 2. \end{matrix} \begin{cases} mg^2 - nh^2 = 1, \\ mg^2 - nh^2 = 2, \end{cases} \qquad \begin{matrix} 3. \\ 4. \end{matrix} \begin{cases} ng^2 - mh^2 = 1, \\ ng^2 - mh^2 = 2, \end{cases}$$

$$\begin{array}{ll} 5. \left\{ \begin{array}{l} h^2 - mng^2 = -1, \\ h^2 - mng^2 = -2, \end{array} \right. & 7. \left\{ \begin{array}{l} g^2 - mnh^2 = 1, \\ g^2 - mnh^2 = 2; \end{array} \right. \\ 6. & 8. \end{array}$$

but of these, the seventh, *viz.* $g^2 - mnh^2 = 1$, cannot have place; because we suppose here, as in the foregoing proposition, that p and q are the least values that satisfy the equation

$$p^2 - aq^2 = 1, \text{ or } p^2 - mnq^2 = 1.$$

Now by means of these decompositions we readily draw the following conclusions:

1. If the numbers m and n are both of the form $4n + 3$, no one of the bottom equations can obtain; for, in this case, whatever forms we give to the two squares g^2 and h^2, the equations will be of one of the forms $4n$, $4n + 1$, $4n + 3$, no one of which can be equal to ± 2. The fifth equation is also impossible on the same supposition; because this, by transposition, gives $\dfrac{h^2 + 1}{mn} = g^2$, an integer, whereas we have shown, that no number that is the sum of two squares prime to each other, can be divided by numbers of the form $4n + 3$ (art. 105, and *lemma* 4, page 200).

There remains, then, only the two equations 1 and 3, one of which must, therefore, necessarily obtain; and hence we draw the following remarkable theorems.

1. *If* m *and* n *be both of the form* 4n + 3, *the equation*

$$mx^2 - ny^2 = \pm 1$$

will be always possible in integer numbers; that is, under one or other of the signs + *or* -1.

If we suppose m and n to be both of the form $4n + 1$, then the same reasoning will apply, except

to the fifth equation, and, therefore, in this case, our theorem must be expressed thus:

2. *If* m *and* n *be both of the form* 4n + 1, *then one of the equations*

$$x^2 - mny^2 = -1, \text{ or } mx^2 - ny^2 = \pm 1,$$

will always be resolvible in integers.

And in a similar manner we may deduce the following theorem, which is still more general.

3. *If* m *and* m′ *be two prime numbers of the form* 4n + 3, *and* n *a prime number of the form* 4n′ + 1, *it will be always possible to satisfy one of the three following equations:*

$$n\,x^2 - mm'y^2 = \pm 1,$$
$$m\,x^2 - m'n\,y^2 = \pm 1,$$
$$m'x^2 - mn\,y^2 = \pm 1,$$

CHAP. II.

On the Solution of Indeterminate Equations of the First Degree.

PROP. I.

159. To find the values of x and y in the equation

$$ax - by = \pm 1.$$

We have already considered this equation (art. 141), and it is only repeated here to preserve uniformity, and to offer a few remarks that could not be properly introduced in that article.

First, it may be observed, that a and b must be prime to each other, for otherwise the equation will be impossible; because the first side of the equation would be divisible by the common divisor of a and b, but the other side ± 1 would not. But, if a and b have these conditions, then the equation is always possible in integer numbers.

Now we have seen, that if $\frac{p^\circ}{q^\circ}, \frac{p}{q}$, be any two consecutive terms of a series of converging fractions, then $p^\circ q - q^\circ p = \pm 1$; and, therefore, to find the values of x and y, in the above equation, we have only to convert $\frac{a}{b}$ into a series of converging fractions, and to assume, for these quantities, the terms

of that, which immediately precedes $\frac{a}{b}$; so shall we have $ax-by=\pm 1$, the upper sign having place when $\frac{y}{x}<\frac{a}{b}$, and the lower when $\frac{y}{x}>\frac{a}{b}$.

Let, then, p and q be the terms of the fraction preceding $\frac{a}{b}$; then, if $aq-bp=-1$, we may convert it into $+1$, by making $x=bm-q$, and $y=am-p$, which evidently gives

$$a(bm-q)-b(am-p)=+1.$$

And, on the contrary, if $aq-bp=+1$, it may be converted to -1, by a similar substitution; and it is evident, that, by means of the indeterminate letter m, an indefinite number of solutions may be obtained in both cases; and when we require no change in the sign, then we have $x=bm+q$, and $y=am+p$.

Ex. 1. Find the values of x and y in the equation

$$15x-17y=1.$$

First, by the rule for continued fractions,

$$\begin{array}{l} 15)17(1 \\ \quad\underline{} \\ \quad\; 2)15(7 \\ \quad\quad\underline{} \\ \quad\quad\; 1)2(2 \end{array}$$

Quotients, 1, 7, 2.

Conv. frac. $\frac{1}{1}$, $\frac{8}{7}$, $\frac{17}{15}$;

whence $p=8$, and $q=7$, which give

$$15p-17q=+1;$$

therefore, the general values of x and y are

$$x=17m+8, \text{ and } y=15m+7;$$

and by assuming $m=0, 1, 2, 3$, &c., we shall have, for the corresponding values of x and y, as follows:

$$x=8, 25, 42, 59, 76, 93, 110, \&c.$$
$$y=7, 22, 37, 52, 67, 82, 97, \&c.$$

Ex. 2. Find the general values of x and y in the indeterminate equation

$$13x-9y=1.$$

Here, by the rule for continued fractions,

```
9)13(1
  4)9(2
    1)4(4
```

Quotients,	1,	2,	4.
Conv. frac.	$\frac{1}{1}$,	$\frac{3}{2}$,	$\frac{13}{9}$.

whence $p=3$, and $q=2$, which gives

$$13q-9p=-1;$$

and, therefore, the general values of x and y are

$$x=9m-2, \text{ and } y=13m-3;$$

and assuming $m=1, 2, 3, 4$, &c., we have the corresponding values of x and y, as follows:

$$x=7, 16, 25, 34, 43, 52, 61, \&c.$$
$$y=10, 23, 36, 49, 62, 75, 88, \&c.$$

These two examples, with what has been before done in the preceding chapter, will be sufficient to render the student ready in the solution of any equation of the above form, which is the more ne-

cessary, as we shall see that every indeterminate equation of the first degree, which has any possible solution, depends upon the solution of the equation

$$ax - by = \pm 1.$$

PROP. II.

160. To find the general values of x and y in the equation

$$ax - by = \pm c.$$

First, with regard to the limits of possibility of this equation, it may be observed, that a and b must be prime to each other, or, if they have a common divisor, c must have the same, for otherwise the equation is impossible; and if each of these quantities have a common divisor, the whole equation may be divided by it, and thus reduced to another, in which a and b are prime among themselves; for, if this cannot be effected, the equation cannot obtain in integers. Supposing, then, a and b to be prime to each other, and q and p the least numbers that fulfil the conditions of the equation

$$aq - bp = \pm 1,$$

determined by the foregoing proposition, then it is evident that we shall have

$$a \,.\, cq - b \,.\, cp = \pm c;$$

making, therefore, $x = cq$, and $y = cp$, we shall have the solution required: but it is obvious that the same result will be obtained by writing $x = mb + cq$, and $y = ma + cp$, which gives also

$$a(mb + cq) - b(ma + cp) = \pm c;$$

where, by means of the indeterminate m, an in-

definite number of values of x and y may be obtained. And we may always convert the value of the equation from $+c$ to $-c$, or from $-$ to $+$, by taking cp and cq negative, and, in this case, m positive, in order that x and y may be so; for, if

$$a.cq-b:cp=+c, \text{ then}$$
$$a(mb-cq)-b(ma-cp)=-c; \text{ and if}$$
$$a.cq-b.cp=-c, \text{ then will}$$
$$a(mb-cq)-b(ma-cp)=+c.$$

So that the general values of x and y are,

$$x=mb\pm cq, \text{ and } y=ma\pm cp,$$

the upper sign having place for cq and cp, when the expression $aq-bp$ has the same sign with c in the given equation, and the lower one when it has a different sign.

Ex. 1. Find the values of x and y in the indeterminate equation

$$9x-13y=10.$$

First, in the equation

$$9q-13p=\pm 1,$$

we have $q=3$ and $p=2$, which gives $+1$, the same sign as 10 in the proposed equation; and, therefore, the general values of x and y are,

$$x=13m+30, \text{ and } y=9m+20.$$

Therefore, assuming successively

$$m=-2, -1, 0, 1, 2, 3, 4, \&c.,$$

we have the following corresponding values of x and y, which are all deduced from the first two, by adding successively to the values of x the coefficient of y, and to y the coefficient of x.

$$x = 4,\ 17,\ 30,\ 43,\ 56,\ 69,\ 82,\ \&c.$$
$$y = 2,\ 11,\ 20,\ 29,\ 38,\ 47,\ 56,\ \&c.$$

Whence we obtain the following solutions:

$$9 \,.\, 4 - 13 \,.\, 2 = 10,$$
$$9 \,.\, 17 - 13 \,.\, 11 = 10,$$
$$9 \,.\, 30 - 13 \,.\, 20 = 10,$$
$$9 \,.\, 43 - 13 \,.\, 29 = 10,$$
&c. &c.

Ex. 2. Find the values of x and y in the indeterminate equation

$$7x - 12y = 19.$$

First, the equation

$$7q - 12p = \pm 1,$$

gives $q = 5$ and $p = 3$, from which is derived

$$7q - 12p = -1,$$

which is a different sign from 19 in the given equation; therefore, the general values of x and y are,

$$x = 12m - 5 \,.\, 19, \text{ and } y = 7m - 3 \,.\, 19; \text{ or}$$
$$x = 12m - 95, \quad \text{and } y = 7m - 57.$$

Whence we obtain the corresponding values of x and y, by assuming

$$m = 9,\ 10,\ 11,\ \&c.;$$

and it is obvious, that we cannot take $m < 9$, because we should then have x and y negative; and these values of x and y are deduced from each other, as in the foregoing example, by simple addition.

$$x = 13,\ 25,\ 37,\ 49,\ 61,\ 73,\ 85,\ \&c.$$
$$y = 6,\ 13,\ 20,\ 27,\ 34,\ 41,\ 48,\ \&c.$$

PROP. III.

161. To find the general values of x and y in the equation

$$ax + by = c,$$

and to ascertain the number of possible solutions, that the equation admits of in integers.

In the foregoing proposition, where the difference of two quantities was the subject of investigation, we found, that the number of solutions was infinite, providing a and b were prime to each other; but when we consider the sum of the two quantities, as in the present case, the number of solutions is always limited, and in many cases the equation is impossible; we have, however, demonstrated (art. 41), that this equation will always admit of at least one solution, if a and b be prime to each other, and $c > ab - (a + b)$; and it is proposed, in the present proposition, to ascertain the exact number of solutions when the equation is possible, and to point out more accurately the limits of possibility.

The solution of the indeterminate equation

$$ax + by = c$$

depends, like that in the foregoing proposition, upon the equation

$$aq - bp = \pm 1,$$

though its connexion with it is not so readily perceived.

For let p and q be the terms of the converging fraction, immediately preceding $\frac{a}{b}$, then we shall always have either

$$aq - bp = 1, \text{ or } bp - aq = 1;$$

and, in this case, it is indifferent which of the two terms is the leading one, because we are only considering the sum

$$ax + by = c.$$

Let, then, $aq - bp = 1$, then we have also

$$a \cdot cq - b \cdot cp = c;$$

and it is evident, that we shall have the same result if we make

$$x = cq - mb, \text{ and } y = cp - ma;$$

for this still gives

$$a(cq - mb) - b(cp - ma) = c:$$

assuming, therefore, for m such a value, that $cp - ma$ may become negative, while $cq - mb$ remains positive, we shall have

$$a(cq - mb) + b(ma - cp) = c;$$

and, consequently, $x = cq - mb$, and $y = ma - cp$; but if m cannot be so taken that $cp - ma$ shall be negative, while $cq - mb$ remains positive, it is a proof that the proposed equation is impossible in integers. And, on the contrary, the equations will always admit of as many solutions in whole numbers, as there may be different values given to m, such that the above conditions may obtain.

And hence we are enabled to determine, *a priori*, the number of solutions, that any proposed equation of the above form will admit of; for, since we must have $cq > mb$, and $cp < ma$, the number of solutions will always be expressed by the greatest integer contained in

$$\frac{cq}{b} - \frac{cp}{a};$$

as is evident, because m must be less than the first of those fractions, and greater than the second; and, therefore, the difference between the integral part of them will express the number of different values of m, except when $\frac{cq}{b}$ is a complete integer, in which case, as $m < \frac{cq}{b}$, we must take the next less integer; or, which is the same, we must consider $\frac{b}{b}$ as a fraction in this case, and reject it; but this must not be done with the other quantity, because $m > \frac{cp}{a}$.

Ex. 1. Required the values of x and y in the equation

$$9x + 13y = 2000,$$

and the number of possible solutions in integers.

First, in the equation

$$9q - 13p = 1,$$

we have at once $p = 2$, and $q = 3$; therefore, the number of solutions will be

$$\frac{2000 \times 3}{13} - \frac{2000 \times 2}{9} = 461 - 444 = 17.$$

Which are readily obtained from the formulæ

$$x = cq - mb, \quad \text{and } y = ma - cp; \text{ or}$$
$$x = 6000 - 13m, \text{ and } y = 9m - 4000;$$

in which, assuming $m = 445$, in order that $9m > 4000$, we shall have the following solutions, each of which is deduced from the preceding one,

by adding successively 9 for the values of y, and subtracting 13 for those of x.

$x = 215,\ 202,\ 189,\ 176,\ 163,\ 150,\ 137,$ &c.
$y = \ \ 5,\ \ 14,\ \ 23,\ \ 32,\ \ 41,\ \ 50,\ \ 59,$ &c.

That is,

$$9 \,.\, 215 + 13 \,.\, 5 = 2000,$$
$$9 \,.\, 202 + 13 \,.\, 14 = 2000,$$
$$9 \,.\, 189 + 13 \,.\, 23 = 2000,$$
&c. &c. &c.

Ex. 2. Let there be proposed the equation

$$11x + 13y = 190$$

to find the number of solutions, and the values of x and y.

First, in the equation

$$11q - 13p = 1,$$

we have $q = 6$, and $p = 5$; therefore,

$$\frac{190 \,.\, 6}{13} - \frac{190 \,.\, 5}{11} = 87 - 86 = 1:$$

whence it follows, that there is only one possible solution, which we readily obtain from the formulæ

$$x = cq - mb, \quad \text{and } y = ma - cp; \text{ or}$$
$$x = 190 \,.\, 6 - 13m, \text{ and } y = 11m - 190 \,.\, 5:$$

where, by taking $m = 87$, in order that $11m > 190 \,.\, 5$, we have $x = 9$, and $y = 7$, which gives

$$11 \,.\, 9 + 13 \,.\, 7 = 190,$$

as was required.

Ex. 3. How many different ways may 1000*l.* be paid in crowns and guineas?

Putting x for the guineas and y for the crowns, and reducing 1000*l.* to shillings, we have

$$21x+5y=20000;$$

and it is required to determine the number of solutions that this equation admits of in integers.

For this purpose we have the equation

$$21q-5p=1,$$

which gives $q=1$, and $p=4$; then we have

$$\frac{cq}{b}-\frac{cp}{a}=\frac{20000}{5}-\frac{80000}{21}=190:$$

that is, 1000*l.* may be paid 190 different ways, by the combination of crowns and guineas. In this example we deduct 1 from the result, because $20000\div 5$ is an integer.

Cor. If it were proposed to pay 1000*l.* in guineas and moidores, then we must have

$$21x+27y=20000,$$

which is an impossible equation; the first side of it being divisible by 3, but the other side not.

PROP. IV.

162. To find the values of x, y, and z, and the number of solutions of any equation of the form

$$ax+by+cz=d.$$

In the first place, we may observe, that, if any one, or more, of the coefficients a, b, or c, be negative, the number of answers is indefinite.

For, let b be negative, then the equation may be put under the form

$$ax+cz=d+by,$$

in which, by means of the indeterminate y, an indefinite number of values may be given to the second side of the equation; and, consequently, also to

x and z: we need, therefore, only consider equations of the form above given, in which the quantities are all connected together by the sign $+$.

Now, in this equation, as in that in the two foregoing propositions, if a, b, and c, have each a common divisor, which d has not, it becomes impossible; but if only two of them, as a and b, have a common divisor, the equation is still possible; but it requires, in this case, some other considerations, which shall be explained at the conclusion of this proposition: we shall, therefore, in the present instance, limit our investigation to the case in which two, at least, of the coefficients are prime to each other.

The solution of the equation

$$ax + by + cz = d$$

depends, like those in the foregoing propositions, upon the solution of the equation

$$aq - bp = 1;$$

for let one of the three terms, as cz, be transposed to the other side of the equation, then we have

$$ax + by = d - cz,$$

in which the values of x and y, as determined in the preceding proposition, will be

$$x = (d - cz)q - mb, \text{ and } y = ma - (d - cz)p;$$

that is, by substituting $(d - cz)$ for c; which is the only respect in which this equation differs from that of the last problem. And here the only limits to be observed are,

$$\text{1st, } cz < d; \qquad \text{2d, } mb < (d - cz)q;$$

$$\text{3d, } ma > (d - cz)p;$$

by attending to which, all the possible values of x, y, and z, may be obtained: but as these questions generally admit of a great number of solutions, the object of inquiry is not so much to find the solutions themselves, as to determine, *a priori*, the number that the equation admits of in integers. Now we have seen (art. 161), that in the equation

$$ax+by=c,$$

the number of solutions is generally expressed by the formula

$$\frac{cq}{b}-\frac{cp}{a},$$

q and p being first determined by the equation

$$aq-bp=\pm 1.$$

If, therefore, in the equation

$$ax+by=d-cz,$$

we make successively $z=1, 2, 3, 4,$ &c., the number of solutions for each value of z will be as below; *viz.*

$ax+by=d-\ c$, num. of solu. $\dfrac{(d-\ c)q}{b}-\dfrac{(d-\ c)p}{a}$,

$ax+by=d-2c$, - - - - $\dfrac{(d-2c)q}{b}-\dfrac{(d-2c)p}{a}$,

$ax+by=d-3c$, - - - - $\dfrac{(d-3c)q}{b}-\dfrac{(d-3c)p}{a}$,

&c. &c.

The sum of which will be the total number that the given equation admits of; and, therefore, in order to find the exact number of solutions in any equation of this kind, we must first ascertain the

sum of all the integral parts of the arithmetical series,

$$\frac{(d-c)q}{b} + \frac{(d-2c)q}{b} + \frac{(d-3c)q}{b} + \frac{(d-4c)q}{b} + \text{\&c. and}$$

$$\frac{(d-c)p}{a} + \frac{(d-2c)p}{a} + \frac{(d-3c)p}{a} + \frac{(d-4c)p}{a} + \text{\&c.:}$$

and the difference of the two will be the exact number of integral solutions.

Now, in both these series, we know the first and last term, and number of terms; for, the general terms being

$$\frac{(d-cz)q}{b}, \text{ and } \frac{(d-cz)p}{a},$$

we shall have the extreme terms by taking the extreme limits of z; that is, $z = 1$ and $z < \frac{d}{c}$; which last value of z also expresses the number of terms in the series.

Hence, then, having the elements of the progression given, we readily find the sums of the two whole series; and if, therefore, we also find the sums of the fractional part of the terms in each, we shall have, by deducting it from the whole sum, that of the integral part of the series, as required. The latter part of this problem is readily effected; for, the denominator in each term being constant, the fractions will necessarily recur in periods, and the number in each can never exceed the denominator: it will, therefore, only be necessary to find the sum of the fractions in one period, which, being multiplied by the number of periods, will give the sum of the fractional part of the terms, and these,

taken from the total sum, will give the sum of the integral part of the series; then, from what has been before observed, the difference of the two sums will be the number of solutions required. It should also be observed, that, when the number of terms does not consist of an exact number of periods of circulation, the remaining terms, or fractions, must be summed by themselves, which is also readily effected, as they will be the same as the leading terms of the first period: and it must also be remembered, that $\frac{b}{b}$ is to be considered as a fraction in the first series, but not $\frac{a}{a}$ in the second, as is explained at page 325.

Ex. 1. Let there be proposed the equation

$$5x+7y+11z=224$$

to find the number of solutions which it admits of in integers.

Here the greatest limit of $z<\frac{224}{11}$ is 20; also in the equation

$$5q-7p=1$$

we have $q=3$, $p=2$, $a=5$, and $b=7$; and, therefore, the two series of which the sums are required, beginning with the least terms, will be

$$\text{1st,}\quad \frac{3.4}{7}+\frac{3.15}{7}+\frac{3.26}{7}+\frac{3.37}{7}+\text{\&c.}\ \frac{3.113}{7}.$$

$$\text{2d,}\quad \frac{2.4}{5}+\frac{2.15}{5}+\frac{2.26}{5}+\frac{2.37}{5}+\text{\&c.}\ \frac{2.113}{5}.$$

The common difference in the first being $\frac{3.11}{7}$, and

in the second $\frac{2.11}{5}$, and the number of terms in each 20; whence we have

930, for the sum of the first, and

868, for the sum of the second.

Also the first period of fractions, in the first series, is

$$\frac{5}{7}+\frac{3}{7}+\frac{1}{7}+\frac{6}{7}+\frac{4}{7}+\frac{2}{7}+\frac{7}{7}=4;$$

and, in the second series, the first period of fractions is,

$$\frac{3}{5}+0+\frac{2}{5}+\frac{4}{5}+\frac{1}{5}=2;$$

$\frac{7}{7}$ being considered as a fraction in the first (art. 162), but not $\frac{5}{5}$ in the second.

Now the number of terms in each series being 20, we have 2 periods and 6 terms of the first series, $=2.4+$ the first 6 fractions $=11$, for the sum of all the fractions; and, therefore, $930-11=919$, which is the exact sum of the integral terms, first series. And, in the second, we have 4 periods, $=4.2=8$: and, therefore, $868-8=860$, the sum of the integral terms of the second series: and hence, according to the rule,

$$919-860=59$$

is the number of integral solutions.

Remark. This example is the same as prob. 11, page 191, Simpson's Algebra, where the number of solutions is said to be sixty; but, upon examination, it appears, that one of the

sixty which he has given cannot obtain; that is, $z=14$, $x=10$, and $y=14$; which error being corrected, gives 59 for the number of solutions, as above.

Ex. 2. Having proposed the equation

$$7x+9y+23z=9999,$$

it is required to determine the number of its solutions in positive integers.

Here the greatest limit of $z<\frac{9999}{23}=434$; also in the equation

$$7q-9p=1,$$

we have $q=4$ and $p=3$, $a=7$ and $b=9$; also

$$9999-23.434=17:$$

therefore, the series whose sums are required are as follow; *viz.*

$$\text{1st, } \frac{4.17}{9}+\frac{4.40}{9}+\frac{4.63}{9}+\text{ \&c. } \frac{4.9976}{9}.$$

$$\text{2d, } \frac{3.17}{7}+\frac{3.40}{7}+\frac{3.63}{7}+\text{ \&c. } \frac{3.9976}{7}.$$

The common difference in the first being

$$\frac{4.23}{9}=10\frac{2}{9};$$

and, in the second,

$$\frac{3.23}{7}=9\frac{6}{7};$$

also the number of terms in each, 434, that being the greatest limit of z.

Hence we have the sum of,

$$\text{First series,} \quad =963769\frac{3}{9};$$

$$\text{Second series,} \quad =929349.$$

Also the first period of fractions in the first series,

$$\frac{5}{9}+\frac{7}{9}+\frac{9}{9}+\frac{2}{9}+\frac{4}{9}+\frac{6}{9}+\frac{8}{9}+\frac{1}{9}+\frac{3}{9}=5:$$

and $\frac{434}{9}=48\frac{2}{9}$, or 48 periods and two terms

$$=5.48+\frac{5}{9}+\frac{7}{9}=241\frac{3}{9}.$$

And, in the second series, the first period of fractions will be

$$\frac{2}{7}+\frac{1}{7}+0+\frac{6}{7}+\frac{5}{7}+\frac{4}{7}+\frac{3}{7}=3;$$

and $\frac{434}{7}=62$, or 62 periods: therefore,

$$62.3=186.$$

Hence,

$963769\frac{3}{9}-241\frac{3}{9}=963528$ {integral terms, first series; and

$929349\ \ -186\ \ =929163$ {integral terms, second series.

Whence the difference, } $=34365$,

is the number of integral solutions required.

163. Cor. We have at present only considered the case in which two, at least, of the given coefficients are prime to each other; and, when this is not the case, the following transformation will be requisite, and which will be better explained by a partial than by a general example.

Let it therefore be proposed to find the number of solutions that the equation

$$12x+15y+20z=100001$$

admits of in positive integers.

By transposing $20z$, and dividing by 3, we have

$$4x+5y=33334-7z+\frac{z-1}{3};$$

and as this last must be an integer, put $\frac{z-1}{3}=u$, or $z=3u+1$, and this being substituted for z, the above equation becomes

$$12x+15y+20(3u+1)=100001;$$

or, dividing by 3, and transposing

$$4x+5y+20u=33327,$$

the number of solutions in which will be the same as in the original one, but in this u may become 0, as we shall in that case have $z=1$.

Now here, the greatest limit of

$$u<\frac{33327}{20}=1666,$$

and the equation

$$5q-4p=1$$

gives $q=1$ and $p=1$; whence the series will each consist of 1667 terms, because u may $=0$, and their sums will be

$$\text{1st, } \frac{7}{4}+\frac{27}{4}+\frac{47}{4}+\frac{67}{4}+ \text{ \&c. } \frac{33327}{4}=6945972\frac{1}{4};$$

$$\text{2d, } \frac{7}{5}+\frac{27}{5}+\frac{47}{5}+\frac{67}{5}+ \text{ \&c. } \frac{33307}{5}=5556777\frac{4}{5};$$

and the fractions of the first series will be

$$\frac{3}{4}+\frac{3}{4}+\frac{3}{4}+ \text{ \&c.};$$

where, each term having the same fraction, the sum will be

$$\frac{3}{4} \times 1667 = 1250\frac{1}{4}.$$

In the second series the fractions are

$$\frac{2}{5} + \frac{2}{5} + \frac{2}{5} + \text{\&c.}$$

the sum being

$$\frac{2}{5} \times 1667 = 666\frac{4}{5};$$

and hence we have

$$6945972\frac{1}{4} - 1250\frac{1}{4} = 6944722,$$

$$5556777\frac{4}{5} - 666\frac{4}{5} = 5556111.$$

$$\left.\begin{array}{l}\text{Whence the total number}\\ \quad\text{of solutions,}\end{array}\right\} = 1388611.$$

When there are four or more unknown quantities, the number of possible solutions is found in a similar manner.

PROP. V.

164. Having given any number of equations less than the number of unknown quantities which enter therein, to determine those quantities.

Let there be proposed the two equations

$$a x + b y + c z = d,$$
$$a' x + b' y + c' z = d';$$

to find the values of x, y, and z.

Multiply the first by a' and the second by a, whence, by subtraction, we obtain

$$(a'b-ab')y+(a'c-ac')z=a'd-d'a;$$

or, dividing each of these known coefficients by its greatest common divisor, if they have any, and representing the results by b'', c'', d'', this equation becomes

$$b''y+c''z=d''.$$

Find now the values of y and z in this equation, and these being substituted for them, in the equation

$$x=\frac{d-cz-by}{a},$$

will give the corresponding values of x; of which those that are fractional must of course be rejected, and also those that render $(cz+by)>d$.

Ex. 1. Giving

$$\begin{cases} 3x+\ \ 5y+\ \ 7z=560, \\ 9x+25y+49z=2920, \end{cases}$$

to find all the integral values of x, y, and z.

Multiplying the first by 3, we have

$$\begin{cases} 9x+15y+21z=1680, \\ 9x+25y+49z=2920, \end{cases}$$

whence, by subtraction, we have

$$10y+28z=1240;$$

or,

$$5y+14z=620:$$

and here the values of y and z are found to be,

$$y=110,\ 96,\ 82,\ 68,\ 54,\ 40,\ 26,\ 12;$$
$$z=\ \ 5,\ 10,\ 15,\ 20,\ 25,\ 30,\ 35,\ 40.$$

And of these the only two that give

$$x=\frac{560-7z-5y}{3},$$

an integer, are the following; *viz.*

$$\begin{cases} z=15, \text{ and } y=82; \text{ whence } x=15, \\ z=30, \text{ and } y=40; \text{ whence } x=50. \end{cases}$$

Remark. Though this method of solution never fails of giving all the possible values of x, y, and z, in equations of this kind, yet we may frequently shorten the operation in particular cases, in the following manner:

Having obtained, as above, the equation

$$5y+14z=620,$$

we have, by division,

$$y=124+3z-\frac{z}{5},$$

so that z must be a multiple of 5; make, then, $z=5u$, and we obtain

$$y=124-14u;$$

which values of y and z, substituted in the first equation, give

$$3x-35u=-60, \text{ or } 3x=35u-60,$$

whence u must be divisible by 3; take, therefore, $u=3t$, and we obtain

$$x=35t-20,\ y=124-42t, \text{ and } z=15t:$$

the value of y limits t not to exceed 2; assuming, therefore, $t=1$ and 2, we have exactly the same solution as above.

PROP. VI.

165. To decompose a given numeral fraction having a composite denominator into a number of simple fractions having prime denominators.

This is in fact only an application of the foregoing propositions to this particular case; for let

$\frac{m}{n}$ be the given fraction, and suppose, in the first instance, that its denominator consists of two prime factors, or $n=ab$, it will then be to find

$$\frac{m}{ab}=\frac{p}{a}+\frac{q}{b}, \text{ or}$$

$$aq+bp=m;$$

in which equation, having determined the values of p and q, we shall have $\frac{p}{a}$ and $\frac{q}{b}$ for the fractions required; and as many different ways may any such fraction be decomposed into others, as the above equation admits of integral solutions.

If the given fraction be $\frac{m}{abc}$, then we may first resolve it into two fractions, and one of these into two others; thus, let

$$\frac{m}{abc}=\frac{p}{ab}+\frac{q}{c},$$

then we have

$$abq+cp=m;$$

and having, from this equation, found the values of p and q, we shall have

$$\frac{m}{abc}=\frac{p}{ab}+\frac{q}{c}.$$

Again, let

$$\frac{p}{ab}=\frac{r}{a}+\frac{s}{b},$$

whence we obtain

$$as+rb=p;$$

find r and s in this equation, so shall we have

$$\frac{m}{abc}=\frac{r}{a}+\frac{s}{b}+\frac{q}{c},$$

as required. And we may proceed in the same manner to decompose any given fraction having a composite denominator.

Ex. 1. Find two fractions, the denominators of which are 5 and 7, whose sum is equal to $\frac{19}{35}$.

Make

$$\frac{p}{7}+\frac{q}{5}=\frac{19}{35},$$

which furnishes the equation

$$5p+7q=19;$$

and here we have $p=1$ and $q=2$: therefore, $\frac{1}{7}$ and $\frac{2}{5}$ are the fractions required; for these give

$$\frac{1}{7}+\frac{2}{5}=\frac{19}{35}.$$

Ex. 2. Find three fractions, the sum of which shall be equal to $\frac{401}{315}$.

Having first found the denominator to be equal to the product of the three factors $5 \cdot 7 \cdot 9$, it follows immediately, that these three numbers must be the denominators of the fractions sought; and if the given fraction cannot be decomposed into three fractions, having these denominators, it is in vain to seek the decomposition in any others.

Supposing, then, in the first place,

$$\frac{p}{35}+\frac{q}{9}=\frac{401}{315},$$

we have

$$9p+35q=401;$$

which give $q=4$ and $p=29$, whence

$$\frac{401}{315}=\frac{29}{35}+\frac{4}{9}.$$

And now, in order to decompose $\frac{29}{35}$, we must have

$$\frac{p'}{7}+\frac{q'}{5}=\frac{29}{35}, \text{ or } 5p'+7q'=29;$$

which gives $q'=2$ and $p'=3$, whence

$$\frac{29}{35}=\frac{2}{5}, \ \frac{3}{7}, \text{ and } \frac{401}{315}=\frac{2}{5}+\frac{3}{7}+\frac{4}{9},$$

as required.

PROP. VII.

166. To find the least number that is contained under two, three, or more given forms; or, which is the same, to find the least number which, being divided by given numbers, shall leave given remainders.

Let

$$N=am+b=a'n+b'=a''p+b''= \&c.$$

it is required to determine the least value of N, that fulfils these conditions. Or, it is required to find the least number N, such that, being divided successively by a, a', a'', &c., the remainders shall be b, b', b'', &c.

First, since $am+b=a'n+b'$, we have

$$am-a'n=b'-b;$$

find, therefore, in this equation, the least values of m and n (by art. 160), then will $am+b$, or $a'n+b'$, express the least number that fulfils the first two conditions: let, now, this number be called c, then it is evident, that every number of the form $aa'q+c$ will also fulfil these conditions, and we must proceed to find

$$aa'q+c=a''p+b'', \text{ or } aa'q-a''p=b''-c;$$

that is, the least values of q and p in this equation, so shall we have $aa'q+c$ for the least number that answers the first three conditions, which, being called d, we shall have $aa'a''r+d$, as a general expression for all numbers of this latter class: and thus we may proceed to any required extent.

Ex. 1. Find the least number which, being divided by 28, 19, and 15, shall leave for remainders respectively 19, 15, and 11.

Here we have

$$28m+19=19n+15=15p+11;$$

now, in the equation

$$19n-28m=4,$$

the least values of m and n are (as determined by art. 160) $m=8$ and $n=12$, whence

$$28m+19=19n+15=243;$$

and we have now to find

$$28.19q+243=15p+11, \text{ or } 532q-15p=-232,$$

in which equation $p=512$ and $q=14$, whence

$$532q+243=15p+11=7691,$$

which is the least number having the required conditions.

Miscellaneous Examples.

1. Find the least values of x and y that fulfil the conditions of the equation

$$19x - 117y = 11.$$

Ans. 56 and 9.

2. Find all the values of x and y that the following equation admits of in integers:

$$13x + 14y = 200.$$

Ans. 10 and 5.

3. Find the integral values of x and y in the equation

$$27x + 39y = 7432,$$

or prove there are no such values.

Ans. Impossible.

4. To find whether the equation

$$7x + 13y = 71$$

is possible or impossible. *Ans.* Impossible.

5. Find two fractions having 5 and 7 for denominators, whose sum is equal to $\frac{26}{35}$.

Ans. $\frac{1}{7}$ and $\frac{3}{5}$.

6. Find three fractions having prime denominators, whose sum is equal to $1\frac{276}{385}$.

Ans. $\frac{3}{5}$, $\frac{4}{7}$, $\frac{6}{11}$.

7. What number is that, which, being divided by 9 and 13, shall leave for remainders 5 and 12?

Ans. 77.

8. Can 100*l.* be paid exactly in the present gold coin of this kingdom? *Ans.* Impossible.

9. Required such values of x and y, in the indeterminate equation

$$7x+19y=1921,$$

that their sum $x+y$ may be the least possible.

Ans. $x=3$ $y=100$.

10. Find how many solutions the equation

$$5x+7y+11z=4000$$

admits of in positive integers.

11. Find such values of x, y, and z, in the equation

$$5x+11y+13z=2000,$$

that their sum $x+y+z$ may be a minimum.

12. Find the least number, that, being divided successively by the nine digits,

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,$$

shall leave respectively for remainders the digits

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8.$$

CHAP. III.

On the Solution of Indeterminate Equations of the Second Degree.

PROP. I.

167. To find the values of x in the indeterminate equation

$$ax^2 + bx + c = z^2.$$

Though this problem fall under the general form of equations that are investigated in the following propositions, yet, as there are some conditions of the coefficients that render the solution more simple than others, it will be proper to state a few of those particulars, without, however, multiplying the rules too much, which would only lead to embarrassment, as it is by far better to employ one general method, that embraces all cases, although the operation may be a little longer, than to give a number of particular rules, suitable only to as many particular conditions. We shall, therefore, consider, in this place, only the three following cases; *viz.* when

$$\begin{cases} c = 0, & \text{or } ax^2 + bx = z^2; \\ a = m^2, & \text{or } m^2x^2 + bx + c = z^2; \\ c = m^2, & \text{or } x^2 + bx + m^2 = z^2. \end{cases}$$

168. Case 1. *To find the value of x in the indeterminate equation*

$$ax^2 + bx = z^2.$$

Here we may assume $z = xy$, and hence we obtain

$$ax^2 + bx = x^2y^2, \text{ or } ax + b = xy^2.$$

Whence $x = \frac{b}{y^2 - a}$, which will become more general by making $y = \frac{p}{q}$; and, substituting this value, we have

$$x = \frac{bq^2}{p^2 - aq^2};$$

in which expression p and q may be taken any integral values at pleasure.

Ex. 1. Required the value of x in the equation

$$5x^2 + 7x = z^2.$$

Here, since $a = 5$ and $b = 7$, the value of x becomes

$$x = \frac{7q^2}{p^2 - 5q^2},$$

in which p and q may be taken any numbers whatever: by assuming $p = 3$ and $q = 1$, we have $x = \frac{7}{4}$, which fraction will be found to answer the required conditions.

Ex. 2. Required the value of x in the equation

$$2x^2 - 3x = z^2.$$

Since $a = 2$ and $b = -3$, we have

$$x = \frac{-3q^2}{p^2 - 2q^2}, \text{ or } x = \frac{3q^2}{2q^2 - p^2}.$$

And, by assuming $q=4$ and $p=5$, we have $x=\frac{48}{7}$, which fraction will be found to answer the required conditions.

In both these examples we have arrived at fractional results; but integral ones may, in all cases, be found, at least whenever b is positive; for, in that case, the denominator is always of the form p^2-aq^2, which we have seen (art. 150) may be made equal to unity; but, when b is negative, this condition is not always possible, because the equation

$$aq^2-p^2=1, \text{ or } p^2-aq^2=-1,$$

is not always resolvible (cor. 1, art. 150).

Ex. 3. Find such integral value of x as will render the equation

$$13x^2+7x=z^2$$

rational.

Here we have from the general solution

$$x=\frac{7q^2}{p^2-13q^2};$$

and, therefore, we must find such values of p and q, that will give

$$p^2-13q^2=1,$$

which, by art. 151, are found to be $p=649$ and $q=180$, whence

$$x=7q^2=7\cdot180^2=226800,$$

which is the least integer having the required conditions.

169. Case 2. *To find the values of x in the indeterminate equation*

$$m^2x^2+bx+c=z^2.$$

Assume $z=mx+y$, then we have

$$m^2x^2+bx+c=m^2x^2+2mxy+y^2.$$

Whence, by cancelling m^2x^2,

$$x=\frac{y^2-c}{b-2my}.$$

Or if, in order to generalize, we make $y=\frac{p}{q}$, this becomes

$$x=\frac{p^2-cq^2}{bq^2-2mpq}.$$

In which expression p and q may be assumed at pleasure.

Ex. 1. Required the value of x in the equation

$$9x^2+7z+5=z^2.$$

Here, since $m=3$, $b=7$, $c=5$, the values of x are contained in the expression

$$x=\frac{p^2-5q^2}{7q^2-6pq};$$

in which, by assuming $p=4$ and $q=2$, we have $x=\frac{4}{20}$, or $\frac{1}{5}$; which fraction answers the condition of the equation.

Ex. 2. Required the value of x in the equation

$$9x^2+5=z^2.$$

Here $m=3$, $b=0$, $c=5$; therefore, the general value of x is

$$x=\frac{p^2-5q^2}{-6pq}, \text{ or } x=\frac{5q^2-p^2}{6pq}.$$

By taking $q=1$ and $p=1$ we have $x=\frac{2}{3}$, which

fraction will be found to answer the required conditions.

170. Case 3. *To find the value of x in the indeterminate equation*

$$ax^2 + bx + m^2 = z^2.$$

Assume $z = m + xy$, then we have

$$ax^2 + bx + m^2 = m^2 + 2mxy + x^2y^2.$$

Whence

$$x = \frac{b - 2my}{y^2 - a}.$$

Which is exactly the reciprocal of the expression deduced for the value of x, in the preceding case, except that we have a instead of c; and if, in order to render it more general, we make $y = \frac{p}{q}$ it becomes,

$$x = \frac{bq^2 - 2mpq}{p^2 - aq^2};$$

which latter equation may always be resolved in integers, because

$$p^2 - aq^2 = 1$$

is always possible (art. 150); and this is true whether b be positive or negative, as we have only, in the latter case, to make either p or q negative; or, which is still the same, assume $z = m - xy$ instead of $z = m + xy$.

Ex. 1. Find the integral value of x in the equation

$$5x^2 + 7x + 1 = z^2.$$

Here we have $a = 5$, $b = 7$, $m = 1$, whence

$$x = \frac{7q^2 - 2pq}{p^2 - 5q^2}.$$

Now, in order that we may have

$$p^2 - 5q^2 = 1,$$

we find, by art. 150, $p=9$ and $q=4$, whence $x=40$, which number will be found to answer the required conditions.

Ex. 2. Find an integer value for x in the equation

$$7x^2 - 5x + 1 = z^2.$$

Since $a=7$, $b=-5$, and $m=1$, we have

$$x = \frac{-5q^2 + 2pq}{p^2 - 7q^2}.$$

And, in order that this denominator may be equal to unity, we must find, by art. 150, the values of p and q, such that this condition may have place, which are $p=8$ and $q=3$; whence is obtained $x=3$, which makes

$$7 \cdot 3^2 - 5 \cdot 3 + 1 = 7^2,$$

as required.

Hence it follows, that when integral values of x are required, we must have particular values of p and q, obtained by means of art. 150, or of the table subjoined to this volume; but when only fractional values are required, then we may assume p and q equal to any numbers at pleasure.

171. Cor. The foregoing solution will hold, whether m be known or unknown; in fact, when m^2 is indeterminate, it may, in the expression

$$x = \frac{bq^2 - 2mpq}{p^2 - aq^2},$$

be assumed at pleasure; and the solution is still more general, if m also enters into the middle term with x; thus, for example, if we write y for m, the equation under the latter supposition will be

$$ax^2 + bxy + y^2 = z^2;$$

which may always be found in integers by assuming

$$\begin{cases} x = 2pq + bq^2, \\ y = \ \ p^2 - aq^2, \end{cases}$$

in which expressions p and q may be assumed at pleasure; and, consequently, integral values obtained for x and y *ad libitum* (art. 101).

Ex. Find the values of x and y in the equation

$$3x^2 + 5xy + y^2 = z^2.$$

Here $a = 3$ and $b = 5$; therefore,

$$\begin{cases} x = 2pq + 5q^2, \\ y = \ \ p^2 - 3q^2. \end{cases}$$

And, assuming $p = 3$ and $q = 1$, we have $x = 11$ and $y = 6$, which values, substituted for x and y in the proposed equation, give

$$3 \, . \, 11^2 + 5 \, . \, 11 \, . \, 6 + 6^2 = 27^2.$$

And other values may be found by changing those of p and q.

If $b = 0$, and the proposed equation be

$$ax^2 + y^2 = z^2,$$

then the values of x and y are

$$\begin{cases} x = 2pq, \\ y = \ \ p^2 - aq^2. \end{cases}$$

Which is exactly the result obtained at cor. 2, art. 54.

Remark. A few other partial rules might have been added here for particular cases or conditions of the coefficients; but, as the principles explained in the following propositions embrace every possible form of equation, a multiplicity of rules for conditional equations seems to be both unnecessary and improper.

PROP. II.

172. Every indeterminate equation of the second degree, containing two unknown quantities, may be reduced to the form

$$u^2 - \text{A}t^2 = \text{B}.$$

Let

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

represent any indeterminate equation of the second degree, in which x and y are the two indeterminates, and a, b, c, d, e, and f, any known integers positive or negative, or zero; then I say, that this equation may, in all cases, be reduced to the more simple form

$$u^2 - \text{A}t^2 = \text{B}.$$

For, first, multiply the proposed equation by $4a$, which makes

$$4ax^2 + 4abxy + 4acy^2 + 4adx + 4aey + 4af = 0;$$

add $b^2y^2 + 2bdy + d^2$ to both sides, and transpose: so shall we have

$$(2ax + by + d)^2 = (by + d)^2 - 4a(cy^2 + ey + f); \text{ or}$$
$$2ax + by + d = \sqrt{\{(by + d)^2 - 4a(cy^2 + ey + f)\}}.$$

And, in order to abridge the latter expression, let

$$\begin{aligned} \sqrt{\{(by + d)^2 - 4a(cy + ey + f)\}} &= t, \\ b^2 - 4ac \text{ - - - - - - - } &= \text{A}, \\ 2bd - 4ae \text{ - - - - - - - } &= 2g, \\ d^2 - 4af \text{ - - - - - - - } &= h; \end{aligned}$$

that is, A will represent the multiples of y^2, $2g$ the multiples of y, and h the absolute quantity which contains no indeterminate letter. Now these sub-

stitutions will furnish the two following equations; *viz.*

$$\begin{cases} 2ax + by \quad + d = t, \\ \text{A}y^2 + 2gy + h = t^2. \end{cases}$$

Multiplying this last by A, we have

$$\text{A}^2y^2 + 2\text{A}gy + \text{A}h = \text{A}t^2;$$

adding g^2, this becomes

$$(\text{A}y + g)^2 = \text{A}(t^2 - h) + g^2, \text{ or}$$
$$(\text{A}y + g)^2 - \text{A}t^2 = g^2 - \text{A}h.$$

Substituting again $\text{A}y + g = u$, and $g^2 - \text{A}h = \text{B}$, we have

$$u^2 - \text{A}t^2 = \text{B};$$

and, therefore, the proposed equation has been transformed, as required.

And it is obvious, that the values of x and y in the proposed equation will be immediately deduced from the solution of the transformed equation

$$u^2 - \text{A}t^2 = \text{B}.$$

For we have

$$\text{A}y + g = u, \text{ or } y = \frac{u - g}{\text{A}}; \text{ and}$$

$$2ax + by + d = t, \text{ or } x = \frac{t - d - by}{2a};$$

or, substituting for y, in this last, we have

$$x = \frac{(t - d)\text{A} - (u - g)b}{2a\text{A}}.$$

And since, in the transformed equation, u and t enter only in the second power, we may take t and u, in these last expressions, of the values of x and y, either positive or negative, at pleasure;

and when the solution of the proposed equation is required only in rational numbers, it is obvious, that we shall have it immediately from any rational values of t and u in the equation

$$u^2 - \text{A}t^2 = \text{B};$$

but if the proposed equation is to be found in integers, then we can only employ such values of t and u as, when substituted in the expression for x and y, render these quantities integral; in consequence of which restriction, the solution, in these cases, is generally very tedious, and frequently impossible.

Ex. 1. Let it be proposed to transform the equation

$$3x^2 + 8xy - 3y^2 + 2x - 5y = 110, \text{ or}$$
$$3x^2 + 8xy - 3y^2 + 2x - 5y - 110 = 0,$$

to another of the form

$$u^2 - \text{A}t^2 = \text{B}.$$

Here

$a = 3$, $b = 8$, $c = -3$, $d = 2$, $e = -5$, $f = -110$.

Whence

$$\left.\begin{array}{l} bd - 2ae = g = 46 \\ d^2 - 4af = h = 1324 \end{array}\right\} \text{ and}$$
$$\left\{\begin{array}{l} b^2 - 4ac = \text{A} = 100 \\ g^2 - ah \ = \text{B} = -130284; \end{array}\right.$$

therefore, the transformed equation is

$$u^2 - 100t^2 = -130284:$$

and, if we had the values of t and u in this equation, those of x and y in the original one would be readily obtained by means of the formulæ

$$y = \frac{u - g}{\text{A}}, \text{ and } x = \frac{t - by - d}{2a};$$

but the solution of the equation

$$u^2 - At^2 = B$$

belongs to the following proposition, the transformation being all that is required in the present case.

Ex. 2. It is required to transform the equation

$$5x^2 + 3x + 7 = y^2, \text{ or}$$
$$5x^2 - y^2 + 3x + 7 = 0,$$

to another of the form

$$u^2 - At^2 = B.$$

Here $a = 5$, $b = 0$, $c = -1$, $d = 3$, $e = 0$, $f = 7$.

Whence we have

$$\left.\begin{array}{l} bd - 2ae = g = 0, \\ d^2 - 4af = h = -131, \end{array}\right\} \text{ and } \left\{\begin{array}{l} b^2 - 4ac = A = 20, \\ g^2 - ah = B = 655; \end{array}\right.$$

therefore, the transformed equation is

$$u^2 - 20t^2 = 655:$$

and the values of u and t being found in this equation, by the method explained in the following proposition, we shall have those of x and y in the one proposed from the expressions

$$y = \frac{u - g}{A}, \text{ and } x = \frac{t - by - d}{2a}.$$

Remark. The general equation above given includes every possible form of an indeterminate equation of the second degree, and we have seen that this is always reducible to the form

$$u^2 - At^2 = B;$$

and, consequently, on the solution of this last depends that of every possible case which can arise in indeterminate equations of this dimension: but

it should be observed, that, in the solution of the equation

$$u^2 - \text{A}t^2 = \text{B},$$

we may have t and u fractional, as $u = \frac{x}{z}$ and $t = \frac{y}{z}$, whence the above becomes

$$\frac{x^2}{z^2} - \text{A}\frac{y^2}{z^2} = \text{B}, \text{ or}$$

$$x^2 - \text{A}y^2 = \text{B}z^2;$$

an equation in which the indeterminates x, y, and z, are all integral, as well as the known quantities A and B; and as all possible cases are reducible to this form, the solution of it becomes the more particularly interesting.

PROP. III.

173. In all cases in which the equation

$$x^2 - \text{A}y^2 = \text{B}z^2$$

is possible, it may be transformed to another of the form

$$x'^2 - y'^2 = \text{C}z'^2.$$

We have already (at art. 53) given a rule for judging of the possibility or impossibility of every equation of the form

$$x^2 - ay^2 = \text{B}z^2,$$

or, more generally, of the form

$$\text{A}x^2 - \text{B}y^2 = \text{C}z^2;$$

but, in that place, we were not able to show the absolute possibility in those cases in which the given equation fell under a possible form; we shall, however, by means of this proposition, show, that every equation falling under a possible form is

really resolvible, and the contrary when it falls under an impossible, which latter part is in fact proved in the article above mentioned.

Having, therefore, first ascertained the possibility of the equation

$$x^2 - \text{A}y^2 = \text{B}z^2,$$

by the proposition above mentioned, the transformation of it to another of the form

$$x'^2 - y'^2 = \text{C}z'^2$$

will be effected in the manner following: but, before entering upon this subject, it will be proper to make a few preliminary observations; *viz.*

1. The indeterminates x, y, and z, may be considered as being prime to each other, as appears from *lemma*, art. 47.

2. The given quantities A and B may be supposed to have no square divisor; for let $\text{A} = \text{A}'k^2$, and $\text{B} = \text{B}'l^2$, then the equation becomes

$$x^2 - \text{A}'(ky)^2 = \text{B}'(lz)^2, \text{ or}$$
$$x^2 - \text{A}'y'^2 = \text{B}'z'^2;$$

by making $ky = y'$, and $lz = z'$, we may, therefore, always consider A and B as containing no square divisor.

3. The indeterminate y is prime to B; for if y and B had a common divisor, x^2 must necessarily have the same; and, therefore, x and y would not be prime to each other, which is contrary to what has been already demonstrated: and the same reasoning is equally applicable to A and z.

4. The quantities A and B may always be supposed positive; for if they be not both positive, the equation may always be transformed to another similar one, in which the resulting quantities, re-

presented by A and B, will be both positive: thus, the only possible cases are the four following; *viz.*

1st, A positive, B positive,
2d, A negative, B negative,
3d, A positive, B negative.
4th, A negative, B positive.

Which give the following four equations:

$$\text{1st,}\quad x^2 - \text{A}y^2 = +\text{B}z^2.$$
$$\text{2d,}\quad x^2 + \text{A}y^2 = -\text{B}z^2.$$
$$\text{3d,}\quad x^2 - \text{A}y^2 = -\text{B}z^2.$$
$$\text{4th,}\quad x^2 + \text{A}y^2 = +\text{B}z^2.$$

Now, I say, that the three latter equations are impossible, or reducible to the first form, in which A and B are both positive.

For the third and fourth equations are exactly similar, by only transposing the quantities $\text{A}y^2$, and $\text{B}z^2$, and each of these is reducible to the first form; for multiply $x^2 + \text{A}y^2 = \text{B}z^2$ by B, and transpose, then it becomes

$$\text{B}^2z^2 - \text{AB}y^2 = \text{B}x^2,$$

which is precisely the form of the first; and the second is evidently impossible from its nature. Hence, therefore, it appears, that if in the proposed equation A and B are not both positive, it may (if it be a possible equation) be transformed to a similar one, in which the resulting quantities, represented by A and B, shall be both positive.

We may, therefore, in what follows, consider A and B as being both positive, as containing neither of them any square divisor; and the three indeterminates x, y, and z, as integers prime to each other; also y prime to B and z prime to A: which being premised, we shall proceed to the

transformation of the given equation, as announced in the head of the proposition.

174. *Transformation of the equation*

$$x^2 - Ay^2 = Bz^2$$

to the form

$$x'^2 - y'^2 = Cz'^2.$$

In the first place, let us suppose $B > A$, for, if it were otherwise, we should have only to put the equation under the form

$$x^2 - Bz^2 = Ay^2,$$

in which we have $A > B$; so that we may always suppose the coefficient of the second side of the equation to be the greatest of the two, unless in case of equality, which case forms a separate proposition.

Let then, in the given equation,

$$x^2 - Ay^2 = Bz^2,$$

$B > A$, and since we have y prime to B, by the foregoing article, we may make $x = ny - By'$ (cor. 1, art. 40), n and y' being two indeterminates; which expression being substituted for x, in the above equation, it becomes

$$n^2y^2 - 2nByy' + B^2y'^2 - Ay^2 = Bz^2;$$

or, dividing by B and transposing,

$$\frac{n^2 - A}{B}y^2 - 2nyy' + By'^2 = z^2;$$

and, since B is prime to y, it is evident, that $n^2 - A$ must be divisible by B, for otherwise the equality could not obtain, all the other part of the equation being integral; in fact, our rule for ascertaining the possibility of the proposed equation (art. 53) depends upon the condition of the equation

$$\frac{n^2 - \text{A}}{\text{B}} = e$$

being an integer: let, then,

$$\frac{n^2 - \text{A}}{\text{B}} = \text{B}'k^2,$$

k^2 being the greatest square contained in the quotient of $\frac{n^2 - \text{A}}{\text{B}}$; and this value being substituted for $\frac{n^2 - \text{A}}{\text{B}}$ in the above equation, gives

$$\text{B}'k^2y^2 - 2nyy' + \text{B}y'^2 = z^2.$$

Now we have before shown (art. 44), that all squares are of the same form to modulus B, as the squares

$$1^2,\ 2^2,\ 3^2,\ \&c.,\ (\tfrac{1}{2}\text{B})^2;$$

and, therefore, the least value of n will never exceed $\frac{1}{2}$B: we shall, therefore, be sure, by trying all the intermediate numbers from 1 to $\frac{1}{2}$B, to fall upon the possible values of n between the limits 1 and $\frac{1}{2}$B, that render the above expression an integer.

Suppose, then, we have found one or many values of n within the above limits, which have the required conditions of rendering $\frac{n^2 - \text{A}}{\text{B}}$ an integer, we must, with each of these values, continue the transformation in the following manner; *viz.*

Repeating again the equation

$$\text{B}'k^2y^2 - 2nyy' + \text{B}y'^2 = z^2,$$

and multiplying by $\text{B}'k^2$, we have

$$B'^2k^4y^2 - 2nB'k^2yy' + B'Bk^2y'^2 \quad = B'k^2z^2, \text{ or}$$
$$(B'k^2y - ny')^2 + B'Bk^2y'^2 - n^2y'^2 = B'k^2z^2;$$

and, since $n^2 - A = B'Bk^2$, this becomes

$$(B'k^2y - ny')^2 - Ay'^2 = B'k^2z^2;$$

or, making $B'k^2y - ny' = x'$, and $k^2z^2 = z'^2$, we have, for the transformed equation,

$$x'^2 - Ay'^2 = B'z'^2,$$

which is exactly similar to the equation first proposed, except that in this $B' < \frac{1}{4}B$, for $n < \frac{1}{2}B$, therefore $n^2 - A < \frac{1}{4}B^2$; and, consequently, since

$$\frac{n^2 - A}{B} = B'k^2,$$

we must have $B' < \frac{1}{4}B$.

We have, therefore, transformed the given equation to a similar and dependent one, of which one of the coefficients is less than in the equation proposed; and if, in this new equation, B' be equal to unity, or to any square, the equation is transposed as required. And the values of x', y', and z', being determined in this, will give us the values x, y, and z, in the original. For we have

1st, $x = ny \quad - By'$.
2d, $x' = B'k^2y - ny'$.
3d, $z' = kz$.

From the second of these we have

$$y = \frac{x' + ny'}{B'k^2},$$

which therefore thus becomes known.

And the first gives

$$x = \frac{x' + ny'}{B'k^2}n - By'.$$

And the third reduces immediately to

$$z = \frac{z'}{k}.$$

But if neither of the above conditions have place, that is, if B′ be neither equal to a square nor to unity, we must first ascertain whether B′ be still $>$ A, and if it be, we may proceed in the same manner to transform this last equation to another similar one,

$$x''^2 - \text{A}y''^2 = \text{B}''z''^2;$$

in which last $\text{B}'' < \frac{1}{4}\text{B}'$: proceeding thus, by successive transformation, we must be finally brought to an equation in which $\text{B}'^{(n)}$ or $\text{C} < \text{A}$.

Having arrived at this equation, by transposing, we shall have

$$x''^2 - \text{C}z''^2 = \text{A}y''^2,$$

in which now, we have $\text{A} > \text{C}$.

If, then, we represent this new equation by

$$x^2 - \text{C}y^2 = \text{A}z^2,$$

we may, by proceeding exactly as above, reduce this to another similar and dependent equation,

$$x'^2 - \text{C}y'^2 = \text{A}^{(m)}z'^2;$$

or, calling $\text{A}^{(m)} = \text{D}$, to this,

$$x'^2 - \text{C}y'^2 = \text{D}z'^2,$$

in which $\text{A}^{(m)}$, or $\text{D} < \text{C}$; or, by transposing,

$$x'^2 - \text{D}z'^2 = \text{C}y'^2,$$

in which $\text{C} > \text{D}$. Representing this anew by

$$x^2 - \text{D}y^2 = \text{C}z^2,$$

we may proceed to reduce it in a similar manner to the preceding one. Since then, at every step, we reduce the coefficients, so that $\text{A} < \text{B}$, $\text{C} < \text{A}$, $\text{D} < \text{C}$, &c., it

is obvious, that we must finally arrive at one that is equal to unity; for it has been seen that these coefficients are always positive, and they can never become $=0$. Now it is impossible for a series of integers to go on continually decreasing, under these conditions, without one of them becoming at last equal to unity; and hence it follows, that when the equation

$$x^2 - Ay^2 = Bz^2$$

is possible, it may always be transformed into another equation of the form

$$x'^2 - y'^2 = Cz'^2,$$

which last equation is always resolvible (by art. 54); and, from the values of the indeterminates in this last equation, we may proceed by successive steps to those of x, y, and z, in the original one proposed, by means of equations analogous to those in the preceding part of this proposition; *viz.*

$$y = \frac{x' + ny'}{B'k^2}.$$

$$x = \frac{x' + ny'}{B'k^2}n - By'.$$

$$z = \frac{z'}{k}.$$

175. From what has been explained in the above article, we derive the following simple method of arriving at the final equation, without absolutely performing the operation, which it was necessary to explain in order to show the principles on which the transformation was effected.

It appears from what has been said, that, in order to effect the successive reductions, we must make the following calculations,

$$x^2 - \text{A}y^2 = \text{B}\,z^2, \qquad \frac{n^2 - \text{A}}{\text{B}} = \text{B}'\,k^2,$$

$$x^2 - \text{A}y^2 = \text{B}'\,z^2, \qquad \frac{n'^2 - \text{A}}{\text{B}'} = \text{B}''\,k'^2,$$

$$x^2 - \text{A}y^2 = \text{B}''z^2, \qquad \frac{n''^2 - \text{A}}{\text{B}''} = \text{B}'''k''^2,$$

$$\&\text{c}. \qquad \&\text{c}.$$

$$x^2 - \text{A}y^2 = \text{B}^{(m)}z^2, \text{ or } \text{C}z^2,$$

till we have $\text{C} < \text{A}$; then, transposing, our calculation must be carried on again in the same manner as above: thus,

$$x^2 - \text{C}y^2 = \text{A}\,z^2, \qquad \frac{n^2 - \text{C}}{\text{A}} = \text{A}'\,l^2,$$

$$x^2 - \text{C}y^2 = \text{A}'\,z^2, \qquad \frac{n'^2 - \text{C}}{\text{A}'} = \text{A}''\,l'^2,$$

$$x^2 - \text{C}y^2 = \text{A}''z^2, \qquad \frac{n''^2 - \text{C}}{\text{A}''} = \text{A}'''l''^2,$$

$$\&\text{c}. \qquad \&\text{c}.$$

$$x^2 - \text{C}y^2 = \text{A}^{(m)}z^2, \text{ or } \text{D}z^2,$$

in which expressions k^2, l^2, &c., are the greatest integral squares in the quotient $\frac{n^2 - \text{C}}{\text{A}}$: which reductions and transformations must be continued, till we arrive at the equation required; that is, in which one of the coefficients above represented by A, B, C, &c., becomes unity; and having found the value of the indeterminates in this last, we shall arrive at those of x, y, and z, in the original equation, by means of equations analogous to the following:

$$y=\frac{x'+ny'}{B'k^2}.$$

$$x=ny-By'.$$

$$z=\frac{z'}{k}.$$

In the above forms, the accents of x, y, and z, are omitted, to avoid confusion; but the reader will be aware that these letters are not of the same value in any two of the preceding equations. It may also be proper to add, farther, that though, in order to show the successive transformations, we have employed several forms, yet there are few practical cases in which these are numerous.

Ex. 1. It is required to transform the equation

$$x^2-5y^2=11z^2$$

to another of the form

$$x'^2-y'^2=cz'^2,$$

and hence to determine the values of x, y, and z, in the equation proposed.

Here we have

$$\frac{n^2-5}{11}=B'k^2=1,$$

by assuming $n=4$, whence $B'=1$; and, therefore, the transformed equation is

$$\begin{cases} x'^2-5y'^2=z'^2, \text{ or} \\ x'^2-z'^2=5y'^2. \end{cases}$$

Now the general values of x' and y' in this equation are (by art. 54)

$$x'=p^2+5m^2=14,$$

$$z'=p^2-5m^2=4,$$

$$y'=2pm \quad\quad =6,$$

that is, by assuming $p=3$ and $m=1$; whence those of x, y, and z, in the equation proposed, are

$$y=\frac{x'+ny'}{\text{B}'k^2}=\frac{14+24}{1}=38,$$
$$x=ny-\text{B}y'=4.38-11.6=86,$$
$$z=\frac{z'}{k}=\frac{4}{1}=4,$$

which numbers answer the required conditions, for

$$86^2-5.38^2=11.4^2.$$

And, by giving different values to p and m, various other integral solutions may be obtained.

Ex. 2. Required the values of x, y, and z, in the equation

$$x^2-12y^2=13z^2.$$

First,

$$\frac{n^2-12}{13}=\text{B}'k^2=1,$$

by assuming $n=5$; whence we have, for the transformed equation,

$$x'^2-12y'^2=z'^2, \text{ or } x'^2-z'^2=12y'^2,$$

in which we readily find $x'=4$, $z'=2$, and $y'=1$; whence

$$y=\frac{x'+ny'}{\text{B}'k^2}=\frac{4+5}{1}=9,$$
$$x=ny-\text{B}y'=5.9-13.1=32,$$
$$z=\frac{z'}{k}=\frac{2}{1}=2,$$

which numbers answer the required conditions, for

$$32^2-12.9^2=13.2^2.$$

In these two examples, we have arrived at the equation required by the first transformation, in which cases we readily find integral values for x, y, and z; but if two or more transpositions be requisite, then we must be satisfied with fractional results, at least we cannot always obtain integral ones, under those conditions.

Ex. 3. Required the values of x, y, and z, in the equation

$$x^2 - 10y^2 = 31z^2.$$

First,

$$\frac{n^2 - 10}{31} = \text{B}'k^2 = 6,$$

by assuming $n = 14$, and thus we have $\text{B}' = 6 \,.\, k^2 = 1$, so that the transformed equation is

$$\begin{cases} x'^2 - 10y'^2 = 6z'^2, \text{ or} \\ x'^2 - 6z'^2 = 10y'^2. \end{cases}$$

Then again,

$$\frac{n'^2 - 6}{10} = \text{C}'l^2 = 1,$$

by assuming $n' = 4$, whence $\text{C} = 1$, and the new transformed equation is

$$\begin{cases} x''^2 - 6z''^2 = y''^2, \text{ or} \\ x''^2 - y''^2 = 6z''^2; \end{cases}$$

in which last we find readily $x'' = 5$, $y'' = 1$, and $z'' = 2$. And having thus obtained the values of the indeterminates in this equation, we readily deduce those of x', y', and z'; and hence again those of x, y, and z, in the equation proposed. Thus,

$$z' = \frac{x'' + n'z''}{c'l^2} = \frac{5 + 4 . 2}{1} = 13,$$

$$x' = n'z' - cz'' = 4 . 13 - 10 . 2 = 32,$$

$$y' = \frac{y''}{l} = \frac{1}{1} = 1:$$

which numbers answer the conditions of the equation

$$x'^2 - 10y'^2 = 6z'^2;$$

and hence again we have

$$y = \frac{x' + ny'}{B'k^2} = \frac{32 + 14 . 1}{6} = \frac{23}{3},$$

$$x = ny - 31y' = 14 . \frac{23}{3} - 31 . 1 = \frac{229}{3},$$

$$z = \frac{z'}{k} = \frac{13}{1} = 13, \text{ or } \frac{39}{3};$$

and these fractions, or their numerators only, will answer the required conditions; for

$$229^2 - 10 . 23^2 = 31 . 39^2.$$

It will be readily observed here, that the first set of equations, whence we derive the values of x', y', z', are exactly analogous to the last, from which we find x, y, and z; the only difference being, that z'' and y'' stand respectively in the place of y' and z' in the preceding one, as must necessarily be the case, because the equation we transformed was

$$x'^2 - 6z'^2 = 10y'^2,$$

in which z' occupies the place that is given to y in the first.

PROP. IV.

176. To find the values of x, y, and z, in the equation

$$x^2 - Ay^2 = Az^2.$$

In the foregoing proposition, we have always supposed one of the coefficients to be greater than the other; and though we may still make use of a similar principle when they are equal, and thus include both these propositions under one, yet, as the present admits of a simple process, it will be better to consider it separately.

Since then

$$x^2 - Ay^2 = Az^2,$$

it follows that x is divisible by A, and as we may always suppose A to contain no square factor, therefore $x = Ax'$, or $x^2 = Ax'^2$; whence we have

$$A^2x'^2 - Ay^2 = Az^2, \text{ or}$$
$$y^2 + z^2 \qquad = Ax'^2:$$

and since here A contains no square factor, x', y, and z, may be considered as prime to each other; because, if they had a common measure, the whole equation might be divided by it, as we have before seen: this then being the case, make

$$y = nz - Ay', \text{ whence}$$
$$\frac{n^2+1}{A}z^2 - 2nzy' + Ay'^2 = x'^2;$$

therefore n^2+1 must be divisible by A, for otherwise the equality cannot obtain: let then

$$\frac{n^2+1}{A} = A'k^2, \text{ or } n^2 + 1 = AA'k^2,$$

which substitution gives

$$A'k^2z^2 - 2nzy' + Ay'^2 = x'^2.$$

Multiply both sides by $A'k^2$, and we have

$$A'^2k^4z^2 - 2A'nk^2zy' + (n^2+1)y'^2 = A'x'^2k^2, \text{ or}$$

$$(Ak^2z - ny')^2 + y'^2 = A'x'^2k^2;$$

or, for the sake of abridging, make

$$A'k^2z - ny' = z', \text{ and } x'^2k^2 = x''^2,$$

and our equation becomes

$$z'^2 + y'^2 = A'x''^2,$$

which is exactly similar to the equation proposed, except that, in this, $A' < \frac{1}{4}A$; and if A' be now unity, the equation is resolved, as we have, in that case, only to find

$$z'^2 + y'^2 = x''^2,$$

the solution of which is given cor. 3, art. 54. But if A' be still > 1, we must proceed in the same manner to reduce it again to a similar equation, in which $A'' < \frac{1}{4}A'$; and it is manifest, that, by thus continually decreasing the values of A, A', A'', &c., we must, at last, arrive at a term equal to unity; and then the equation will be transformed, as required. And from the values of the indeterminates in this last equation, we arrive, by successive steps, to those of x, y, and z, in the equation proposed, for in each of these we shall have analogous equations to those first obtained; *viz.*

$$y = nz - Ay', \text{ whence } z = \frac{z' + ny'}{A'k^2};$$

$$z' = A'k^2z - ny', \text{ - - - } y = nz - Ay';$$

$$x'k = x'' \text{ - - - } x' = \frac{x''}{k} \text{ and } x = Ax'.$$

Ex. 1. Find the values of x, y, and z, in the equation

$$x^2 - 13y^2 = 13z^2.$$

First, making $x = 13x'$, the above equation becomes, after division,

$$y^2 + z^2 = 13x'^2; \text{ also}$$

$$\frac{n^2+1}{13} = \text{A}'k^2 = 2;$$

by assuming $n = 5$; whence $\text{A}' = 2$, and $k^2 = 1$, so that the transformed equation will be

$$y'^2 + z'^2 = 2x''^2.$$

Now here we have a known case, namely, when $y' = 1$, $z' = 1$, and $x'' = 1$; whence again

$$z = \frac{z' + ny'}{\text{A}k^2} = \frac{1 + 5 . 1}{2} = 3,$$

$$y = nz - \text{A}y' = 5 . 3 - 13 . 1 = 2;$$

$$x' = \frac{x''}{k} = \frac{1}{1} = 1;$$

and, consequently, $x = 13x' = 13$, $y = 2$, and $z = 3$, are the values of x, y, and z, required for

$$13^2 - 13 . 2^2 = 13 . 3^2.$$

177. *Scholium.* This problem may also be resolved upon principles entirely different from the foregoing; for it is demonstrated (art. 105), that the sum of two squares can only be divided by numbers that are also the sums of two squares; and, consequently, when the equation is reduced to the form

$$y^2 + z^2 = \text{A}x'^2,$$

it is evident, that both A and x'^2 are the sums of two squares, because $y^2 + z^2$ is divisible by each of

those quantities; and, farther, it has been shown (art. 91), that the product of two numbers, each the sum of two squares, is of the same form. Hence, then, we have the following solution: assume $A = p^2 + q^2$, and $x'^2 = p'^2 + q'^2$, then will

$$(p^2 + q^2) \times (p'^2 + q'^2) = (pp' \pm qq')^2 + (pq' \mp p'q)^2;$$

that is,

$$(pp' \pm qq')^2 + (pq' \mp p'q)^2 = Ax'^2;$$

and, consequently,

$$\begin{cases} y = pp' \pm qq', \\ z = pq' \mp p'q. \end{cases}$$

In which expressions p and q are known, being the roots of any two squares, of which A is the sum, and p' and q' must be such, that $p'^2 + q'^2 = x'^2$, any square; that is (by cor. 3, art. 54),

$$\begin{cases} p' = m^2 - n^2, \\ q' = 2mn, \end{cases}$$

with which values any equation of this kind may be solved; and it is obvious, if A be not a number of the form $p^2 + q^2$, that the proposed equation is impossible, either in integers or fractions.

Ex. 1. Required the values of x, y, and z, in the equation

$$y^2 + z^2 = 65x^2.$$

From the foregoing formulæ we have

$$\begin{cases} y = pp' \pm qq', \\ z = pq' \mp p'q. \end{cases}$$

Also,

$$65 = 8^2 + 1^2 = 7^2 + 4^2;$$

therefore, $p = 8$ and $q = 1$, or $p = 7$ and $q = 4$.

Again,

$$\begin{cases} p' = m^2 - n^2 = 3, \quad 5, \text{ \&c.,} \\ q' = 2mn \quad\;\; = 4, \; 12, \text{ \&c.;} \end{cases}$$

by assuming $m=2$ $n=1$, $m=3$ $n=2$, &c.

Now these values, substituted for p, q, p', q', in the above formulæ, give the following results:

$$\begin{cases} y = 28, \; 20; \; 37, \;\; 5; \; 52, \;\; 28, \text{ \&c.} \\ z = 29, \; 35; \; 16, \; 40; \; 91, \; 101, \text{ \&c.} \\ x = \;5, \;\; 5; \;\; 5, \;\; 5; \; 13, \;\; 13, \text{ \&c.} \end{cases}$$

Each of which sets of numbers will answer the required conditions of the equation.

Cor. 1. The same principle is equally applicable to the solution of certain other forms of equation; *viz.* to the following:

$$x^2 + y^2 = \text{A}z^2,$$
$$x^2 + 2y^2 = \text{A}z^2,$$
$$x^2 - 2y^2 = \text{A}z^2,$$
$$x^2 + 3y^2 = \text{A}z^2,$$
$$x^2 - 5y^2 = \text{A}z^2,$$

For as these formulæ can only be divided by numbers of the same form as themselves (art. 105, *et seq.*); therefore, when any of these are possible, A is of the same form as the first side of the corresponding equation, z^2 being likewise so; and then again, the multiplication of two formulæ of this kind, as

$$(p^2 \pm aq^2)(p'^2 \pm aq'^2) = x^2 \pm ay^2:$$

that is, they give a product of the same form.

Hence, then, representing the above equations by the general form

$$x^2 + ay^2 = \text{A}z^2,$$

the solution may be obtained as follows: Find

$$\begin{cases} p^2 + aq^2 = A, \\ p'^2 + aq'^2 = z^2, \end{cases}$$

the latter of which equations is readily found by art. 54, and the former is always possible if the equation be so; and having thus found the values of p, q, p', and q', we shall have

$$(p^2 + aq^2)(p'^2 + aq'^2) = Az^2 =$$
$$(pp' \pm aqq')^2 + a(pq' \mp p'q)^2.$$

Whence again we derive, by comparison,

$$\begin{cases} x = pp' \pm aqq', \\ y = pq' \mp p'q. \end{cases}$$

Ex. 1. Required the values of x, y, and z, in the equation

$$x^2 + 2y^2 = 6z^2.$$

Here, A is of the form $x^2 + 2y^2$, for

$$A = 6 = 2^2 + 2 \cdot 1^2;$$

therefore, $p = 2$ and $q = 1$.

Also, assuming $z^2 = 3^2$, we have

$$z^2 = 3^2 = 1 + 2 \cdot 2^2;$$

therefore, $p' = 1$ and $q' = 2$.

Whence,

$$\begin{cases} x = pp' \pm 2qq' = 6, \text{ or } 2; \\ y = pq' \mp \ qp' = 3, \text{ or } 5. \end{cases}$$

Which numbers answer the required conditions; for,

$$\begin{cases} 6^2 + 2 \cdot 3^2 = 6 \cdot 3^2, \\ 2^2 + 2 \cdot 5^2 = 6 \cdot 3^2. \end{cases}$$

And various other values might be found by assuming any other square for z^2, which has the

form $p'^2 + 2q'^2$; and this may always be done by squaring any number of the same form.

Ex. 2. Required the values of x, y, and z, in the equation

$$x^2 - 5y^2 = 11z^2.$$

Here, A being of the form $x^2 - 5y^2$, or

$$A = 11 = 4^2 - 5 \cdot 1^2;$$

therefore, $p = 4$ and $q = 1$.

Also, assuming $z^2 = 2^2$, we have

$$z^2 = 2^2 = 3^2 - 5 \cdot 1^2;$$

therefore, $p' = 3$ and $q' = 1$.

Whence,

$$\begin{cases} x = pp' \pm 5qq' = 17, \text{ or } 7; \\ y = pq' \pm \;\; qp' = \;\; 7, \text{ or } 1. \end{cases}$$

Which numbers give the following results:

$$\begin{cases} 17^2 - 5 \cdot 7^2 = 11 \cdot 2^2, \\ \;\; 7^2 - 5 \cdot 1^2 = 11 \cdot 2^2. \end{cases}$$

And various other values might be obtained, by assuming other squares for $z^2 = p'^2 - 5q'^2$.

It will be observed here, that the ambiguous signs in the compound expressions for x and y are $\pm$ and $\mp$ in the first example, but $\pm$ and $\pm$ in the second; that is, the ambiguous signs are $\pm$ and $\mp$, when the connecting sign is $+$ in the proposed equation, but $\pm$ and $\pm$ when that sign is $-$: the reason for which change will become obvious by considering the nature of the two products.

Cor. 2. In the above equations, we know immediately, from the form of A, whether the equations proposed be possible or impossible; as in the former case, A must have the same form as the first side of the equation with which it is connected,

at least with an exception in the two last, when A is even (see art. 108 and 109). And thus far these equations may be considered as forming a separate class, but in other respects the same principles may be employed for any equation whatever; that is, when A is of the same form as the first side of the equation in which it enters; but when it is not of that form, it does not imply the impossibility of the proposed expression, as is the case in those we have been considering.

PROP. V.

178. Every equation of the form

$$x^2 - Ay^2 = Bz^2,$$

in which $\frac{m^2 - B}{A}$, and $\frac{n^2 - A}{B}$, are both integers, is resolvible in rational numbers.

We have before investigated this theorem (art. 53), but it will be observed, the rule thence deduced, although perfectly correct, is deficient in this, that it is not demonstrated, when an equation falls under a possible form, that it admits of a rational solution; the only certain conclusions being with regard to impossible forms: it is therefore proposed, in the present proposition, to supply this defect, by demonstrating the absolute possibility in the former case, the truth of which, or of the above theorem, results as an immediate consequence of the transformations effected in the preceding propositions, and the demonstration of art. 52. But in order to render the investigation as simple and conclusive as possible, it will be

proper to resume here the forms of reduction, as in art. 175; *viz.*

$$\begin{array}{l|l} x^2 - Ay^2 = Bz^2, & \dfrac{n^2 - A}{B} = B'k^2, \\ x^2 - Ay^2 = B'z^2, & \dfrac{n'^2 - A}{B'} = B''k'^2, \\ & \text{\&c.} \qquad \text{\&c.} \\ x^2 - Ay^2 = B^{(m)}z^2, \text{ or } Cz^2, & \end{array}$$

In which last equation, $B^{(m)}$, or $C < A$.

Then again,

$$\begin{array}{l|l} x^2 - Cy^2 = Az^2, & \dfrac{n^2 - C}{A} = A'l^2, \\ x^2 - Cy^2 = A'z^2, & \dfrac{n'^2 - C}{A'} = A''l'^2, \\ & \text{\&c.} \qquad \text{\&c.} \\ x^2 - Cy^2 = A^{(m)}z^2, \text{ or } Dz^2, & \end{array}$$

till we have $D < C$; and so on, as has been before explained, in art. 175, k^2, k'^2, &c., l^2, l'^2, &c., being, as in that article, the greatest squares contained in the respective quotients, arising from the division of $n^2 - A$, $n^2 - C$, &c., by B, A, &c. And it is to be demonstrated, in the present proposition, that, if it be possible to find $\dfrac{m^2 - B}{A}$, and $\dfrac{n^2 - A}{B}$, both integers, that all the other above analogous forms are also possible in integers; and, therefore, that the equation

$$x^2 - Ay^2 = Bz^2$$

is reducible to a dependent equation of the form

$$x'^2 + y'^2 = Cz^2,$$

in which last form the solution may always be ob-

tained, and whence the values of x, y, and z, in the original equation, also become known.

Now, first, if

$$\frac{n^2 - A}{B} = B'k^2,$$

we have evidently, by transposition,

$$\frac{n^2 - A}{B'} = Bk^2;$$

but if $\frac{n^2 - A}{B'}$ be an integer, so likewise is

$$\frac{(n - uB')^2 - A}{B'},$$

where the indeterminate u may be so assumed, that

$$(n - uB') < \tfrac{1}{2}B';$$

therefore, calling $(n - uB') = n'$, we have

$$\frac{n'^2 - A}{B'} = B''k'^2;$$

and, consequently,

$$\frac{n'^2 - A}{B''} = B'k'^2,$$

an integer; and here again we have also

$$\frac{(n' - uB'')^2 - A}{B''},$$

an integer; or, making $n' - uB'' = n''$,

$$\frac{n''^2 - A}{B''} = B'''k''^2,$$

an integer, and so on, for as many transformations as are requisite; that is, if $\frac{n^2 - A}{B}$ gives an integral quotient, so likewise will all the other analogous forms

$$\frac{n'^2 - \text{A}}{\text{B}'}, \ \frac{n''^2 - \text{A}}{\text{B}''}, \ \&c.$$

till we arrive at

$$\frac{\mu^2 - \text{A}}{\text{B}^{(n)}} = \text{C}.$$

And it therefore now only remains to be shown, that, if $\frac{m^2 - \text{B}}{\text{A}}$ be an integer, $\frac{m^2 - \text{C}}{\text{A}}$ is so likewise; for, this being demonstrated, it will follow, from what is shown above, that the analogous forms

$$\frac{m'^2 - \text{C}}{\text{A}'}, \ \frac{m''^2 - \text{C}}{\text{A}''}, \ \&c.$$

will also give integral quotients; and, therefore, that the possibility of the original equation depends upon the two conditions of

$$\frac{n^2 - \text{A}}{\text{B}}, \text{ and } \frac{m^2 - \text{B}}{\text{A}},$$

being integral.

In order to demonstrate this, let us repeat again our first equations,

$$\begin{array}{llll}
\frac{n^2 - \text{A}}{\text{B}} = \text{B}'k^2, & \text{whence} & \frac{n^2 - \text{B}\,\text{B}'\,k^2}{\text{A}} = 1; \\
\frac{n'^2 - \text{A}}{\text{B}'} = \text{B}''k'^2, & - - - & \frac{n'^2 - \text{B}'\,\text{B}''\,k'^2}{\text{A}} = 1; \\
\frac{n''^2 - \text{A}}{\text{B}''} = \text{B}'''k'^2, & - - - & \frac{n''^2 - \text{B}''\text{B}'''k''^2}{\text{A}} = 1; \\
\&c. \quad \&c. & - - - & \&c. \qquad \&c. \\
\frac{\mu^2 - \text{A}}{\text{B}^{(n)}} = \text{C}k^2, & - - - & \frac{\mu^2 - \text{B}^{(n)}\text{C}k^2}{\text{A}} = 1;
\end{array}$$

and, consequently, $\text{BB}'k^2$, $\text{B}'\text{B}''k'^2$, $\text{B}''\text{B}'''k''^2$, &c., are found amongst the remainders of the squares

$$n^2, \; n'^2, \; n''^2, \; \&c.$$

to modulus A; that is,

$$p\text{A} + \text{BB}'k^2, \; p'\text{A} + \text{B}'\text{B}''k'^2, \; \&c.$$

are all possible forms, when compared with A as a modulus. But we have demonstrated, that the product of a possible and impossible form always produces an impossible form (art. 52), therefore, B and B′ must be of the same kind, with regard to possible or impossible, to modulus A; for if B was a possible remainder to modulus A, and B′ an impossible, then would $\text{BB}'k^2$ be also impossible, as is evident from the proposition above quoted: but we have seen that $\text{BB}'k^2$ is a possible remainder, and, consequently, B and B′ are both of the same kind, as to possible or impossible, to modulus A. And, in the same way, we shall have B″ of the same kind to B′, and, therefore, also to B; and the same of the other quantities B″, B‴, &c. to C: therefore, if $\dfrac{m^2 - \text{B}}{\text{A}}$ be an integer, or

$$m^2 = p\text{A} + \text{B},$$

we shall have also

$$\mu^2 = p\text{A} + \text{C};$$

and the same reasoning will apply to every transformation. Now, since the solution of the proposed equation,

$$x^2 - \text{A}y^2 = \text{B}z^2,$$

depends upon its transformation to the form

$$x'^2 - y'^2 = \text{C}z'^2;$$

and this transformation depending upon the possibility of the integral quotients above stated; also

these having their possibility involved in those of the two conditions

$$\frac{n^2 - A}{B}, \text{ and } \frac{m^2 - B}{A},$$

being integers: it follows, that when these two obtain, the solution of the proposed equation may always be obtained in rational numbers.—Q. E. D.

Cor. And in the same manner it may be shown, that the equation

$$Ax^2 - By^2 = Cz^2$$

is always possible, if it falls under a possible form, according to the method employed at art. 53.

Lemma.

179. We have, in the foregoing propositions, given a general method for solving all possible indeterminate equations of the second degree, and of ascertaining their impossibility when they admit of no rational solution; and, in the following article, it will be shown, how, from one known case, an infinite number of others may be obtained; but, before we proceed to this, it will be advantageous to the reader to collect, under one point of view, all that has been demonstrated in this and the foregoing chapter relating to the equation

$$x^2 - Ny^2 = \pm A.$$

First, then, it has been demonstrated, in art. 105, that the equation

$$x^2 - Ny^2 = +1$$

is always resolvible in integers, providing N be not an exact square. As to the equation

$$x^2 - Ny^2 = -1,$$

it is only resolvible in certain cases; that is, when the fractions arising from $\sqrt{N}$ recur in periods, consisting of an odd number of terms. Also the equation

$$x^2 - Ny^2 = +A$$

is always possible, if A be found in the denominator of any of the complete quotients arising from the $\sqrt{N}$; but the equation

$$x^2 - Ny^2 = -A$$

is only possible when A is found in the denominator of one of the complete quotients, that occupies an even place; and, consequently, the corresponding fraction an odd place. In all these cases, however, if there be one solution possible, there are an indefinite number of others; and, in the following propositions, it is proposed to find general expressions in which the values of x and y are contained for each of the above cases.

PROP. VI.

180. To find the general values of x and y in the equation

$$x^2 - Ny^2 = \pm 1,$$

from the values of p and q in the equation

$$p^2 - Nq^2 = \pm 1.$$

The present problem divides itself into three cases, on account of the ambiguous sign $\pm$, which are as follow; *viz.* To find the values of x and y in the expression $x^2 - Ny^2$, under the following conditions:

1st, $x^2-Ny^2=1$, from the known case $p^2-Nq^2=\quad 1$;
2d, $x^2-Ny^2=1$, - - - - - - - $p^2-Nq^2=-1$;
3d, $x^2-Ny^2=-1$, - - - - - - $p^2-Nq^2=-1$.

Case 1. Resolve the two equations

$$p^2-Nq^2=1, \text{ and } x^2-Ny^2=1,$$

into the factors

$$\begin{cases}(p+q\sqrt{N})(p-q\sqrt{N})=1,\\(x+y\sqrt{N})(x-y\sqrt{N})=1;\end{cases}$$

then we have also

$$(p+q\sqrt{N})^m(p-q\sqrt{N})^m=1^m=1:$$

equating these with the factors in x and y, we obtain

$$x+y\sqrt{N}=(p+q\sqrt{N})^m,$$
$$x-y\sqrt{N}=(p-q\sqrt{N})^m.$$

Whence again, by addition and subtraction,

$$x=\frac{(p+q\sqrt{N})^m+(p-q\sqrt{N})^m}{2},$$

$$y=\frac{(p+q\sqrt{N})^m-(p-q\sqrt{N})^m}{2\sqrt{N}};$$

which values of x and y will always be integral, and will, therefore, be the general values sought; and these are evidently infinite in number, because m is indefinite.

Case 2. The same method may be followed here as in the preceding case, except that the powers represented by the exponent m must be even, in order to convert -1 into $+1$, as is obvious from inspection; and, therefore, the general values of x and y, in this case, are

$$x=\frac{(p+q\sqrt{N})^{2m}+(p-q\sqrt{N})^{2m}}{2},$$

$$y = \frac{(p+q\sqrt{N})^{2m} - (p-q\sqrt{N})^{2m}}{2\sqrt{N}}.$$

Case 3. Here again we have evidently the same result as in the former cases, except that the powers of m must now be odd, for every odd power of $-1 = -1$; therefore, the values of x and y are now

$$x = \frac{(p+q\sqrt{N})^{2m+1} + (p-q\sqrt{N})^{2m+1}}{2},$$

$$y = \frac{(p+q\sqrt{N})^{2m+1} - (p-q\sqrt{N})^{2m+1}}{2\sqrt{N}}.$$

The number of values of x and y being indefinite, as in the former cases.

Let us now illustrate these rules by a few examples.

Ex. 1. In the equation

$$p^2 - 14q^2 = 1,$$

having given $p = 15$ and $q = 4$, to find the general values of x and y in the equation

$$x^2 - 14y^2 = 1.$$

Here, making $m = 2$, we have

$$x = \frac{(15+4\sqrt{14})^2 + (15-4\sqrt{14})^2}{2} = 449,$$

$$y = \frac{(15+4\sqrt{14})^2 - (15-4\sqrt{14})}{2\sqrt{14}} = 120;$$

which give

$$449^2 - 14 \, . \, 120^2 = 1:$$

and other values may be found by assuming any other power instead of the second.

Ex. 2. Given $p = 4$ and $q = 1$, in the equation

$$p^2 - 17q^2 = -1,$$

to find the values of x and y in the equation

$$x^2-17y^2=+1.$$

Here we have again

$$x=\frac{(4+\sqrt{17})^2+(4-\sqrt{17})^2}{2}=33,$$

$$y=\frac{(4+\sqrt{17})^2-(4-\sqrt{17})^2}{2\sqrt{17}}=8;$$

whence

$$33^2-17.8^2=1;$$

and other values may be found by assuming any other even power instead of the second.

Cor. This method of deducing the values of x and y in the equation

$$x^2-\text{N}y^2=1,$$

from those of p and q in the equation

$$p^2-\text{N}q^2=-1,$$

is very useful in finding those values of x and y, being much more ready than continuing the extraction by continued fractions; because, whenever the *minus* sign arises, it always happens before the *plus* sign; this will be evident from the following example.

Ex. 3. To find the values of x and y in the equation

$$x^2-13y^2=1.$$

We find in five terms, proceeding by continued fractions, that, in the equation

$$p^2-13q^2=-1,$$

$p=18$ and $q=5$; therefore, without pursuing the extraction any farther, we have, by means of the above formulæ,

$$x = \frac{(18+5\sqrt{13})^2 + (18-5\sqrt{13})^2}{2} = 649,$$

$$y = \frac{(18+5\sqrt{13})^2 - (18-5\sqrt{13})^2}{2\sqrt{13}} = 180;$$

which, as we observed above, is a much readier method than carrying on the extraction, as in ex. 3, art. 151.

Ex. 4. Given $p=4$ and $q=1$, in the equation

$$p^2 - 17q^2 = -1,$$

to find the values of x and y in the equation

$$x^2 - 17y^2 = -1.$$

Assume,

$$x = \frac{(4+\sqrt{17})^3 + (4-\sqrt{17})^3}{2} = 268,$$

$$y = \frac{(4+\sqrt{17})^3 - (4-\sqrt{17})^3}{2\sqrt{17}} = 67;$$

whence

$$268^2 - 17.67^2 = -1:$$

and other values may be found by assuming any other odd powers instead of the third.

PROP. VII.

181. To find the general values of x and y in the equation

$$x^2 - \text{N}y^2 = \pm \text{A},$$

A being $< \sqrt{\text{N}}$.

We have already shown how the first values of x and y are to be obtained (art. 154), and shall therefore now suppose that these values are known, or that we have found the values of m and n in the equation

$$m^2 - \text{N}n^2 = \pm \text{A};$$

and also those of p and q in the equation

$$p^2 - Nq^2 = \pm 1.$$

Then it is obvious, that

$$(p^2 - Nq^2) \times (m^2 - Nn^2) = \pm A;$$

but, by art. 95,

$$(p^2 - Nq^2) \times (m^2 - Nn^2) =$$

$$\begin{cases} (pm + Nqn)^2 - N(pn + qm)^2, \text{ or} \\ (pm - Nqn)^2 - N(pn - qm)^2; \end{cases}$$

whence we have, for the values of x and y,

$$\begin{cases} x = pm \pm Nqn, \\ y = pn \pm qm. \end{cases}$$

But the general values of p and q in the equation

$$p^2 - Nq^2 = \pm 1,$$

are, by the foregoing proposition,

$$p' = \frac{(p + q\sqrt{N})^m + (p - q\sqrt{N})^m}{2},$$

$$q' = \frac{(p + q\sqrt{N})^m - (p - q\sqrt{N})^m}{2\sqrt{N}},$$

m being even or odd, as the case requires; which general values of p and q, being transferred to the formulæ

$$\begin{cases} x = pm \pm Nqn, \\ y = pn \pm qm, \end{cases}$$

will furnish the general values of x and y in the equation proposed.

Cor. If the known case be

$$p^2 - Nq^2 = -A,$$

and we wish to deduce from this

$$x^2 - Ny^2 = +A,$$

we must find p and q in the equation

$$p^2 - Nq^2 = -1;$$

and then

$$\begin{cases} x = pm \pm Nqn, \\ y = pn \pm qm, \end{cases}$$

will be the values of x and y required.

And generally, if the known case have a different sign from the equation proposed, then we must employ the equation

$$p^2 - Nq^2 = -1.$$

But if it have the same sign, the equation

$$p^2 - Nq^2 = +1$$

is that from which the general values of x and y are to be obtained.

Ex. 1. Having given the values of m and n in the equation

$$m^2 - 7n^2 = 2;$$

viz. $m = 3$ and $n = 1$, to find generally the values of x and y in the equation

$$x^2 - 7y^2 = 2.$$

First, in the equation

$$p^2 - 7q^2 = 1,$$

we have $p = 8$ and $q = 3$; whence the above formulæ give

$$\left.\begin{array}{l} x = pm \pm Nqn, \\ y = pn \pm qm; \end{array}\right\} \text{ that is, } \begin{cases} x = 3, \text{ or } x = 45; \\ y = 1, \text{ or } y = 17; \end{cases}$$

and it is obvious, that, by finding the other values of p and q in the equation

$$p^2 - 7q^2 = 1,$$

we should readily deduce those of x and y in the equation proposed; but it is perhaps as well to consider the values of x and y just found, as new values of m and n, and then we have immediately

$$\left.\begin{array}{l} x = pm \pm \text{N}qn, \\ y = pn \pm qm; \end{array}\right\} \text{ or } \left\{\begin{array}{l} x = 717, \\ y = 271; \end{array}\right.$$

and so on for other values, *ad infinitum.*

Ex. 2. Find the general values of x and y in the equation

$$x^2 - 13y^2 = -3;$$

having given those of m and n in the equation

$$m^2 - 13n^2 = 3;$$

viz. $m = 4$ and $n = 1$.

In this equation, since the absolute quantity has a different sign from the known case, we must employ the equation

$$p^2 - 13q^2 = -1,$$

which gives $p = 18$ and $q = 5$; whence

$$\left.\begin{array}{l} x = pm \pm \text{N}qn, \\ y = pn \pm qm\ ; \end{array}\right\} \text{ that is, } \left\{\begin{array}{l} x = 7, \text{ or } 137; \\ y = 2, \text{ or } \ \ 38; \end{array}\right.$$

which are two of the values sought, for

$$\left\{\begin{array}{r} 7^2 - 13\,.\ 2^2 = -3, \\ 137^2 - 13\,.\,38^2 = -3; \end{array}\right.$$

and other values are readily found, as in the foregoing example.

PROP. VIII.

182. To find general and rational values of x and y in the equation

$$x^2 - \text{N}y^2 = \pm \text{A},$$

A being any number whatever.

In this case we have no direct method of finding integral values for x and y, as we had in the foregoing propositions, unless A fall within the limits prescribed in the last problem, in which case the

solution belongs properly to that article, and we have, therefore, in this place, only to attend to the case in which $A > \sqrt{N}$.

Now if A, though greater than $\sqrt{N}$, be made up of any number of factors, as A', A'', A''', &c., each of which is less than the $\sqrt{N}$, the solution of the equation

$$x^2 - Ny^2 = \pm A,$$

when it is possible, may be deduced from those of the equations

$$\begin{aligned} m^2 - Nn^2 &= \pm A', \\ m'^2 - Nn'^2 &= \pm A'', \\ m''^2 - Nn''^2 &= \pm A''', \\ \&c. \quad & \quad \&c. \end{aligned}$$

because the continued product of factors, each of the above form, is itself also of the same form (art. 95); and we shall therefore have

$$(m^2 - Nn^2)(m'^2 - Nn'^2)(m''^2 - Nn''^2) = x^2 - Ny^2 = \pm A,$$

where the values of x and y will be always determinate, and integral functions of

$$m, n; \ m', n'; \ m'', n'', \&c.$$

For, by the same article,

$$(m^2 - Nn^2) \times (m'^2 - Nn'^2) =$$
$$(mm' \pm Nnn')^2 - N(mn' \pm m'n)^2.$$

And making now

$$\begin{cases} mm' \pm Nnn' = P, \\ mn' \pm m'n = Q, \end{cases}$$

we have

$$(m^2 - Nn^2)(m'^2 - Nn'^2) = P^2 - NQ^2.$$

Again,

$$(P^2 - NQ^2)(m''^2 - Nn''^2) =$$
$$(Pm'' \pm NQn'')^2 - N(Pn'' \pm Qm'')^2;$$

making, therefore,

$$\begin{cases} \text{P}m'' \pm \text{NQ}n'' = x, \\ \text{P}n'' \pm \text{Q}\,m'' = y, \end{cases}$$

we have

$$(m^2 - \text{N}n^2)(m'^2 - \text{N}n'^2)(m''^2 - \text{N}n''^2) = x^2 - \text{N}y^2 = \pm \text{A}.$$

Also, substituting for P and Q, in the foregoing values of x and y, we obtain

$$\begin{cases} x = m''(mm' \pm \text{N}nn') \pm \text{N}n''(mn' \pm m'n), \\ y = n''\,(mm' \pm \text{N}nn') \pm \;m''(mn' \pm m'n). \end{cases}$$

Whence x and y are determinate and integral functions of

$$m,\ n;\ m',\ n';\ m'',\ n'';\ \&c.;$$

which are known integral quantities.

Having thus found one integral value of x and y in the equation

$$x^2 - \text{N}y^2 = \pm \text{A},$$

we shall have the general values of those quantities from the equation

$$p^2 - \text{N}q^2 = \pm 1,$$

as in the foregoing propositions; that is, calling the values of x and y, found as above, m and n, the general values of x and y will be

$$x = pm \pm \text{N}qn,$$
$$y = pn \pm qm;$$

the general values of p and q being expressed by

$$p' = \frac{(p + q\sqrt{\text{N}})^m + (p - q\sqrt{\text{N}})^m}{2},$$

$$q' = \frac{(p + q\sqrt{\text{N}})^m - (p - q\sqrt{\text{N}})^m}{2\sqrt{\text{N}}};$$

the indeterminate power m being even or odd, as the case may require.

Ex. 1. Required the values of x and y in the equation

$$x^2-13y^2=-9.$$

First, having resolved -9 into the factors $+3\times-3$, we must find the values of m and n, and m' and n', in the two equations

$$\begin{cases} m^2-13n^2=+3, \\ m'^2-13n'^2=-3; \end{cases}$$

and also the values of p and q, in the equation

$$p^2-13q^2=1,$$

and then the general values of x and y may be determined as above; thus, in the present case, we have, from example 2 of the foregoing proposition, $m=4$ $n=1$, $m'=7$ $n'=2$; whence the first values of x and y are

$$\begin{cases} x=mm'\pm\text{N}nn'=2, \text{ or } 54; \\ y=m'n\pm mn'=1, \text{ or } 15. \end{cases}$$

And by means of these values, and those of p and q, in the equation

$$p^2-13q^2=\pm1,$$

an indefinite number of other values may be obtained, as in the last proposition.

PROP. IX.

183. To find rational values of x and y in the equation

$$x^2-\text{N}y^2=\pm\text{A},$$

in those cases in which A cannot be resolved into such factors as was supposed in the last article.

When in the equation

$$x^2-\text{N}y^2=\pm\text{A},$$

A is $> \sqrt{N}$, and cannot be resolved into factors, each of which is less than $\sqrt{N}$, we have no general method of solution for integral values; in fact, the equation will not always admit of such values, although there may be fractional ones that will obtain, which is not the case if $A < \sqrt{N}$, or resolvible into factors that are $< \sqrt{N}$. We must, therefore, in this case, employ a different method of solution; that is, we must find the values of t and u in the equation

$$t^2 - Nu^2 = \pm Az^2,$$

by art. 176, and then, dividing the whole by z^2, we have

$$\frac{t^2}{z^2} - N\frac{u^2}{z^2} = \pm A;$$

or, making $\frac{t}{z} = m$ and $\frac{u}{z} = n$, this equation becomes

$$m^2 - Nn^2 = \pm A;$$

and, calling this the known case, we shall have the general values of x and y, by means of the equation

$$p^2 - Nq^2 = \pm 1,$$

as in the foregoing article; that is,

$$\begin{cases} x = pm \pm Nqn, \\ y = pn \pm pm; \end{cases}$$

only in this, the general values may be fractional instead of being integral, as in the former case.

Hence it appears, that in all cases when one solution is given, as many others may be deduced from it as we please; and when the given case is integral, all the other solutions will also be integral;

and when the first is fractional, all the other dependent solutions will be fractional likewise.

Cor. The methods that have been explained, in the preceding proposition, for finding the general values of x and y in equations of the form

$$x^2 - \text{N}y^2 = \text{A},$$

are equally applicable to equations of the form

$$x^2 - \text{N}y^2 = \text{A}z^2,$$

as is evident; because this equation being multiplied by

$$p^2 - \text{N}q^2 = 1,$$

will leave the second side of it the same as at first.

Practical Examples.

1. Find the least integral values of x and y in the indeterminate equation

$$x^2 - 5y^2 = 1.$$

Ans. $x = 9$; $y = 4$.

2. Find the integral values of x, y, and z, in the indeterminate equation

$$x^2 - 5y^2 = 13z^2,$$

or prove that there are no such values.

Ans. Impossible.

3. Required to ascertain the possibility or impossibility of the equation

$$5x^2 - 7y^2 = 11z^2.$$

Ans. Impossible.

4. Find the least integral values of x and y in the indeterminate equation

$$x^2 - 7y^2 = 1,$$

and also in the equation

$$x^2-7y^2=-1,$$

if the latter be possible.

Ans. $\begin{cases} x=8,\ y=3, & \text{1st equation.} \\ \text{Impossible,} & \text{2d equation.} \end{cases}$

5. Find the two least integral values of x and y in the equation

$$x^2-13y^2=1.$$

Ans. $\begin{cases} x=649,\ 842431; \\ y=180,\ 233640. \end{cases}$

6. Find the least values of x and y in the equation

$$x^2-13y^2=4.$$

Ans. $\begin{cases} x=119, \\ y=\ 33. \end{cases}$

7. Required the least integral square that, when multiplied by 113, shall exceed another integral square by unity.

Ans. $\begin{cases} x=1204353, \\ y=\ \ 99296. \end{cases}$

8. Required the least values of x and y in the equation

$$79x^2-101y^2=1.$$

CHAP. IV.

On the Solution of Indeterminate Equations of the Third Degree, and those of Higher Dimensions.

PROP. I.

184. To find rational values of x in the equation

$$ax^3+bx^2+cx+d=z^2.$$

It is only under one partial condition of the absolute term d, that this equation admits of a direct solution, that is, when d is a complete square, as $d=f^2$, in which case the equation becomes

$$ax^3+bx^2+cx+f^2=z^2;$$

and, when this condition has not place, we have no other method of proceeding but by trial; and even when it has, we can find but one solution at a time, which is obtained in the following manner:

1*st Method.* Assume

$$z=f+\frac{c}{2f}x;$$

then, by squaring, we have

$$ax^3+bx^2+cx+f^2=f^2+cx+\frac{c^2}{4f^2}x^2, \text{ or}$$

$$ax^3+bx^2=\frac{c^2}{4f^2}x^2; \text{ whence,}$$

$$x=\frac{c^2-4bf^2}{4af^2}.$$

Ex. 1. Required the value of x in the equation

$$x^3 + x^2 + 3x + 1 = z^2.$$

Here $a=1$, $b=1$, $c=3$, and $f=1$; therefore,

$$x = \frac{c^2 - 4bf^2}{4af^2} = \frac{5}{4},$$

which value, substituted for x, gives $z^2 = (\frac{23}{8})^2$, as required.

2d Method of finding the value of x in the equation

$$ax^3 + bx^2 + cx + f^2 = z^2.$$

Assume

$$z = f + gx + hx^2;$$

then, by squaring, we have

$$ax^3 + bx^2 + cx + f^2 =$$
$$f^2 + 2fgx + (g^2 + 2fh)x^2 + 2hgx^3 + h^2x^4.$$

Now make

$$\begin{cases} 2fg = c, \\ g^2 + 2fh = b, \end{cases}$$

and there will remain

$$ax^3 = 2hgx^3 + h^2x^4; \text{ or}$$

$$x = \frac{a - 2hg}{h^2}.$$

But the two preceding equations give

$$g = \frac{c}{2f}, \text{ and}$$

$$h = \frac{4f^2b - c^2}{8f^3}.$$

Which values, being substituted for h and g, in the above expression for x, give

$$x = \frac{8af^4 - 4bcf^2 + c^3}{(4bf^2 - c^2)^2} \times 8f^2.$$

Ex. 2. Required the value of x in the equation

$$-5x^3+6x^2-4x+1=z^2.$$

Here we have $a=-5$, $b=6$, $c=-4$, and $f=1$; which values, substituted in the above expression, give $x=-1$, which number answers the conditions of the question.

If we employ the formula obtained by the preceding method; *viz.*

$$x=\frac{c^2-4bf^2}{4af^2},$$

we find $x=\frac{2}{5}$, which also answers the required conditions.

Remark. It should be observed, that though these two methods generally give different results, yet, when one of them fails (as is the case when $b=0$ and $c=0$ at the same time), the other fails also; and we must then have recourse to the method that is explained in the following propositions: but even this cannot be employed unless we know one case in which the equation obtains.

PROP. II.

185. Having given the value of m in the equation

$$am^3+bm^2+cm+d=f^2$$

to find the values of x in the indeterminate equation

$$ax^3+bx^2+cx+d=z^2.$$

Assume $y+m=x$, then we have

$$\begin{cases} ay^3 + 3amy^2 + 3am^2y + am^3 = ax^3, \\ \quad - \quad - \quad by^2 + 2bmy + bm^2 = bx^2, \\ \quad - \quad - \quad - \quad - \quad - \quad cy + cm = cx, \\ \quad - \quad - \quad - \quad - \quad - \quad - \quad - \quad d = d. \end{cases}$$

Whence,

$$ay^3 + (3am + b)y^2 + (3am^2 + 2bm + c)y + f^2 = z^2.$$

Or, writing

$$\begin{cases} a \quad - \quad - \quad - \quad - \quad = a', \\ (3am + b) \quad - \quad = b', \\ (3am^2 + 2bm + c) = c'. \end{cases}$$

We have

$$a'y^3 + b'y^2 + c'y + f^2 = z^2.$$

Which being thus reduced to the form of the equation in the preceding case, its solution may be obtained by either of the methods there given; *viz.*

$$y = \frac{c'^2 - 4b'f^2}{4a'f^2}, \text{ or}$$

$$y = \frac{8a'f^4 - 4b'c'f^2 + c'^3}{(4b'f^2c' - c'^2)^2} \times 8f^2.$$

And having found the value of y in this last, we shall have $x = y + m$; and, therefore, x, in the proposed equation, will thus become known.

Ex. 1. Required the value of x in the equation

$$x^3 + 3 = z^2.$$

Here the known case is $m = 1$, which gives

$$1^3 + 3 = 2^2,$$

therefore $f = 2$; also $a = 1$, $b = 0$, $c = 0$, $d = 3$.

And, applying these values as above, we have

$$\begin{cases} a \quad - \quad - \quad - \quad - \quad = a' = 1, \\ (3am + b) \quad - \quad = b' = 3, \\ (3am^2 + 2bm + c) = c' = 3. \end{cases}$$

Whence the new equation is

$$y^3 + 3y^2 + 3y + 4 = z^2.$$

And the value of y, by the first formula of the preceding proposition, is

$$y=\frac{c^2-4bf^2}{4af^2}=\frac{9-48}{16}=\frac{-39}{16}.$$

Therefore,

$$x=y+m=\frac{-39}{16}+1=\frac{-23}{16},$$

the value sought.

Ex. 2. Required the value of x in the equation

$$3x^3+1=z^2.$$

Here we have a known case, $m=1$, which gives

$$3m^3+1=f^2=4,$$

therefore $f=2$; also $a=3$, $b=0$, $c=0$, and $d=1$; and hence

$$\begin{cases} a \quad - \quad - \quad - \quad =a'=3, \\ 3am+b \quad - \quad =b'=9, \\ 3am^2+2bm+c=c'=9. \end{cases}$$

Whence the new equation is

$$3y^3+9y^2+9y+4=z^2.$$

And here the value of y by the first formula (art. 184) is

$$y=\frac{c^2-4bf^2}{4af^2}=\frac{-21}{16}.$$

And, consequently,

$$x=m+y=1+\frac{-21}{16}=\frac{-5}{16}.$$

Which value of x will be found to answer the required conditions of the equation proposed.

If we had employed the second formula instead of the first, we should have found

$$y=\frac{-1952}{1323} \text{ and } x=\frac{-629}{1323}.$$

And it is obvious, that we might now consider either of these results as the value of m in the known case, and thus proceed to find other values of x, providing the equation admitted of more answers. But this is not always the case, as it often happens that from one known value of x we cannot derive another; and this is still not owing to any defect in the method we employ, for it is demonstrable, that some of these equations admit of only one answer; such is, for example, the equation

$$x^3+1=z^2,$$

which obtains when $x=2$; but there is no other value of x, either integral or fractional, that will fulfil the conditions of the equation, as may be demonstrated on similar principles to those employed in Part I. chap. v.

PROP. III.

186. To find rational values of x in the indeterminate equation

$$ax^4+bx^3+cx^2+dx+e=z^2.$$

This proposition, like the preceding one, only admits of a direct solution in particular cases; *viz.*

1st, When e is a complete square, as $e=f^2$.
2d, When a is a complete square, as $a=m^2$.
3d, When both the foregoing conditions obtain.

And when no one of these circumstances has place, a direct solution cannot be obtained, there being, in fact, no other means of proceeding but by trial; if, however, in this way, one solution is

found, a variety of others may commonly be deduced from the one known case, as is shown in the following proposition.

187. Case 1. *To find a rational value of x in the indeterminate equation*

$$ax^4+bx^3+cx^2+dx+f^2=z^2.$$

Assume

$$z=px^2+qx+f;$$

then, by squaring, we have

$$\begin{aligned}&p^2x^4+2pqx^3+(q^2+2pf)x^2+2qfx+f^2=\\&ax^4+\quad bx^3+\qquad\qquad cx^2+\quad dx+f^2.\end{aligned}$$

And now, by making

$$\begin{cases}2qf=d,\\ q^2+2pf=c,\end{cases}$$

we have

$$p^2x^4+2pqx^3=ax^4+bx^3, \text{ or}$$
$$(p^2-a)x^4=(b-2pq)x^3.$$

Whence, from the latter equation,

$$x=\frac{b-2pq}{p^2-a}.$$

But the preceding equation gives

$$q=\frac{d}{2f}, \text{ and } p=\frac{c-q^2}{2f}, \text{ or}$$

$$p=\frac{4cf^2-d^2}{8f^3}.$$

Which values being substituted in the foregoing expression for x, we have

$$x=\frac{(8bf^4-4cdf^2+d^3)8f^2}{16c^2f^4-64af^6-8cd^2f^2+d^4};$$

and this formula will always render the proposed equation a square.

Ex. 1. Required the value of x in the equation

$$x^4+x^3+x^2+x+1=z^2.$$

Here, since $a=1$, $b=1$, $c=1$, $d=1$, and $f=1$, we have

$$x=\frac{-40}{55}=\frac{-8}{11},$$

which fraction, being substituted for x, gives

$$z^2=(\frac{101}{121})^2,$$

as required.

Ex. 2. Required the value of x in the equation

$$2x^4-3x+1=z^2.$$

Here we have $a=2$, $b=0$, $c=0$, $d=-3$, and $f=1$; whence

$$x=\frac{216}{47},$$

which fraction, being substituted for x, will be found to answer the required conditions.

188. Case 2. *To find a rational value of x in the indeterminate equation*

$$m^2x^4+bx^3+cx^2+dx+e=z^2.$$

Assume

$$z=mx^2+px+q;$$

then, by squaring, we have

$$\begin{array}{l} m^2x^4+2mpx^3+(p^2+2mq)x^2+2pqx+q^2= \\ m^2x^4+\quad bx^3+\qquad\qquad\quad cx^2+\quad dx+e. \end{array}$$

And here, making

$$\begin{cases} 2mp=b, \\ p^2+2mq=c, \end{cases}$$

there remains

$$2pqx+q^2=dx+e.$$

Whence, by transposition and division,

$$x = \frac{q^2 - e}{d - 2pq}.$$

Also, from the preceding equations is obtained

$$p = \frac{b}{2m}, \text{ and } q = \frac{c - p^2}{2m}, \text{ or}$$

$$q = \frac{4cm^2 - b^2}{8m^3}.$$

Which values of p and q, being substituted in the above expression for x, we have

$$x = \frac{16c^2m^4 - 64em^6 - 8cb^2m^2 + b^4}{(8dm^4 - 4cbm^2 + b^3)8m^2}.$$

Ex. 3. Required the value of x in the equation

$$x^4 - 3x + 2 = z^2.$$

Here $m = 1$, $b = 0$, $c = 0$, $d = -3$, and $e = 2$; whence

$$x = \frac{2}{3},$$

which fraction, being substituted for x, will be found to answer the required conditions.

Remark. It will readily be observed, that the above formula fails, as does also that obtained in case 1, when the second and fourth terms are wanted, that is, when $b = 0$ and $d = 0$, for in this case the denominator becomes zero, and the value of x infinite, so that in equations of the form

$$m^2x^4 + cx^2 + e = z^2, \text{ and}$$
$$ax^4 + cx^2 + f^2 = z^2,$$

we have no method of solution, although they fall under the form we have been considering; and indeed it frequently happens that such equations

are impossible, as may be demonstrated on other principles: thus, the equation

$$x^4 - x^2 + 1 = z^2$$

is impossible, either in integers or fractions, and several others. But in many cases x has a real value, though we have no other means of arriving at it but by trials; and in this manner we must proceed under every form of the general equation except those of the three cases pointed out in the leading part of this proposition.

189. Case 3. *To find rational values of x in indeterminate equations of the form*

$$m^2x^4 + bx^3 + cx^2 + dx + f^2 = z^2.$$

This equation belongs to each of the foregoing cases, and may therefore be solved by either of the formulæ above given, and it also admits of other solutions, distinct from both of them, which are as follow:

1*st Method of solving the indeterminate equation*

$$m^2x^4 + bx^3 + cx^2 + dx + f^2 = z^2.$$

Assume

$$z = mx^2 + qx + f;$$

then, by squaring, we have

$$\begin{aligned} &m^2x^4 + 2mqx^3 + (q^2 + 2mf)x^2 + 2qfx + f^2 = \\ &m^2x^4 + bx^3 \quad + \quad cx^2 + \quad dx + f^2. \end{aligned}$$

Where, by making $d = 2qf$, or $q = \dfrac{d}{2f}$, there remains

$$bx^3 + cx^2 = 2mqx^3 + (q^2 + 2mf)x^2.$$

Whence,

$$x = \frac{q^2 + 2mf - c}{b - 2mq}.$$

Or, by substituting for q its equivalent $\frac{d}{2f}$, this expression becomes

$$x=\frac{d^2+8mf^3-4cf^2}{4bf^2-4mdf}, \text{ or}$$

$$x=\frac{d^2-8mf^3-4cf^2}{4bf^2+4mdf}.$$

Here the last formula arises from supposing f negative, which may always be done, because it enters into the original equation only in the second power, and therefore f itself may be either $+$ or $-$.

Ex. 1. Required the value of x in the equation

$$4x^4+3x+1=z^2.$$

Here we have $m=2$, $b=0$, $c=0$, $d=3$, and $f=1$; therefore,

$$x=\frac{d^2+8mf^3-4cf^2}{4bf^2-4mdf}=\frac{-25}{24},$$

$$x=\frac{d^2-8mf^3-4cf^2}{4bf^2+4mdf}=\frac{-7}{24},$$

both of which fractions answer the required conditions, the former making

$$z^2=(\frac{926}{576})^2,$$

and the latter, on the same principles, giving

$$z^2=(\frac{447}{576})^2.$$

2d Method of solving the indeterminate equation

$$m^2x^4+bx^3+cx^2+dx+f^2=z^2.$$

Assume

$$z=mx^2+qx+f,$$

as before; by which means we have again

$$m^2x^4 + 2mqx^3 + (q^2 + 2mf)x^2 + 2qfx + f^2 =$$
$$m^2x^4 + \quad bx^3 + \qquad cx^2 + \quad dx + f^2.$$

And now, making $b = 2mq$, or $q = \frac{b}{2m}$, we have

$$cx^2 + dx = (q^2 + 2mf)x^2 + 2qfx.$$

Whence,

$$x = \frac{d - 2qf}{q^2 + 2mf - c}.$$

Or, by substituting for q its equal $\frac{b}{2m}$, this formula becomes

$$x = \frac{4m^2d - 4mbf}{b^2 + 8m^3f - 4m^2c}, \text{ or}$$
$$x = \frac{4m^2d + 4mbf}{b^2 - 8m^3f - 4m^2c},$$

the second formula being obtained as before, by supposing f negative.

Ex. 2. Required the values of x in the equation

$$x^4 - 3x + 4 = z^2.$$

Here $m = 1$, $b = 0$, $c = 0$, $d = -3$, and $f = 2$; therefore,

$$x = \frac{4m^2d - 4mbf}{b^2 + 8m^3f - 4m^2c} = \frac{-3}{4},$$
$$x = \frac{4m^2d + 4mbf}{b^2 - 8m^3f - 4m^2c} = \frac{+3}{4},$$

either of which fractions, substituted for x, will be found to answer the required conditions.

Remark. It will be observed again here, that the formulæ which we have thus found, all fail under the same circumstances as before; *viz.* when $b = 0$ and $d = 0$: we must, therefore, in all such cases,

endeavour to find one value of x by trials; and, if this cannot be done, then it is in vain to attempt the solution of the equation, which, as we before observed, may not admit of one; but, if one value can be found under any circumstance, then we may deduce others from this one, as in the following proposition.

PROP. IV.

190. Having given the value of m in the equation

$$am^4 + bm^3 + cm^2 + dm + e = f^2,$$

to find values for x in the indeterminate equation

$$ax^4 + bx^3 + cx^2 + dx + e = z^2.$$

Assume $y + m = x$, then we have

$$\begin{array}{rl} ay^4 + 4amy^3 + 6am^2y^2 + 4am^3y + am^4 &= ax^4, \\ - \; - \; by^3 + 3bmy^2 + 3bm^2y + bm^3 &= bx^3, \\ - \; - \; - \; - \; - \; cy^2 + 2cmy + cm^2 &= cx^2, \\ - \; - \; - \; - \; - \; - \; - \; dy + dm &= dx \\ - \; - \; - \; - \; - \; - \; - \; - \; - \; - \; e &= e. \end{array}$$

And now, writing

$$\begin{array}{ll} a \; - \; - \; - \; - \; - \; - \; - \; - \; - & = a', \\ 4am + b \; - \; - \; - \; - \; - \; - \; - \; - & = b', \\ 6am^2 + 3bm + c \; - \; - \; - \; - \; - & = c', \\ 4am^3 + 3bm^2 + 2cm + d \; - \; - \; - & = d', \\ am^4 + bm^3 + cm^2 + dm + e \; - & = f^2. \end{array}$$

we have

$$ax^4 + bx^3 + cx^2 + dx + e = z^2, \text{ or}$$
$$a'y^4 + b'y^3 + c'y^2 + d'y + f^2 = z^2.$$

And now, the last term of this formula in y

being a square, we have, by case 1 of the preceding proposition,

$$y = \frac{(8b'f^4 - 4c'd'f^2 + d'^3)8f^2}{16c'^2f^4 - 64a'f^6 - 8c'd'^2f^2 + d'^4};$$

and, consequently, since $x = y + m$, we shall have the value of x as required.

Ex. 1. Required the value of x in the equation

$$5x^4 - 1 = z^2,$$

the known case being $m = 1$, which, in the equation

$$5m^4 - 1 = f^2,$$

gives $f^2 = 2^2$.

Here we have $a = 5$, $b = 0$, $c = 0$, $d = 0$, and $e = -1$; therefore, $a' = 5$, $b' = 20$, $c' = 30$, $d' = 20$, $f = 2$; whence

$$y = \frac{(8b'f^4 - 4c'd'f^2 + d'^3)8f^2}{16c'^2f^4 - 64a'f^6 - 8c'd'^2f^2 + d'^4} = \frac{-24}{11},$$

and

$$x = y + m = \frac{-24}{11} + 1 = \frac{-13}{11}.$$

And, since x enters only in the fourth power, we may likewise take x positive as well as negative; and, therefore, the value of x sought is

$$x = \pm\frac{13}{11},$$

which fraction will be found to answer the required conditions, making

$$z^2 = (\frac{358}{121})^2.$$

Ex. 2. Required the value of x in the equation

$$2x^4 - 1 = z^2.$$

Here we have a known case, *viz.* $m = 1$, and $f = 1$;

therefore, since $a=2$, $b=0$, $c=0$, $d=0$, $f=1$, and $m=1$, we have $a'=2$, $b'=8$, $c'=12$, $d'=8$, and $f=1$; whence

$$y=\frac{(8b'f^4-4c'd'f^2+d'^3)8f^2}{16c'^2f^4-64a'f^6-8e'd'^2f^2+d'^4}=12;$$

and, consequently, $y+m$, or $x=12+1=13$; which may be taken either $+$ or -1, because only the fourth power of x enters into the proposed equation, and this number answers the required conditions for

$$2.13^4-1=(239)^2.$$

We might now, in both the foregoing examples, consider these known values of x as new values of m, and thus proceed to find others; but it is obvious that we should soon be led to very complicated fractions, which would render the practical operation very laborious.

PROP. V.

191. To find rational values of x in the indeterminate equation

$$ax^3+bx^2+cx+d=z^3.$$

This equation, in its present general form, will not admit of a direct solution, this being only obtainable under the three following conditions; *viz.*

Case 1. When d is a complete cube, or $d=f^3$.

Case 2. When a is a complete cube, or $a=m^3$.

Case 3. When both these conditions have place.

192. Case 1. *To find the value of x in the indeterminate equation*

$$ax^3+bx^2+cx+f^3=z^3.$$

Assume

$$px+f=z;$$

then, by cubing, we have

$$\begin{aligned}p^3x^3+3p^2fx^2+3pf^2x+f^3=\\ ax^3+\quad bx^2+\quad cx+f^3.\end{aligned}$$

And now, making $3pf^2=c$, or $p=\frac{c}{3f^2}$, we obtain

$$ax^3+bx^2=p^3x^3+3p^2fx^2, \text{ or}$$

$$x=\frac{3p^2f-b}{a-p^3}.$$

And, by substituting here the above value of p, this expression becomes

$$x=\frac{(c^2-3bf^3)9f^3}{27af^6-c^3}.$$

Ex. 1. Required the value of x in the equation

$$3x^3+2x+1=z^3.$$

Here $a=3$, $b=0$, $c=2$, and $f=1$; whence

$$x=\frac{(c^2-3bf^3)9f^3}{27af^6-c^3}=\frac{36}{73},$$

which fraction answers the required conditions for

$$3(\frac{36}{73})^3+2(\frac{36}{73})+1=(\frac{97}{73})^3.$$

Ex. 2. Required the value of x in the equation

$$x^3-5x-1=z^3.$$

Here $a=1$, $b=0$, $c=-5$, and $f=-1$; therefore,

$$x=\frac{(c^2-3bf^3)9f^3}{27af^6-c^3}=\frac{-225}{152},$$

which fraction answers the required conditions, making

$$z^3=(\frac{223}{152})^3.$$

193. Case 2. *To find the value of x in the indeterminate equation*

$$m^3x^3+bx^2+cx+d=z^3.$$

Assume

$$z=mx+p;$$

then, by cubing, we have

$$m^3x^3+3m^2px^2+3mp^2x+p^3=$$
$$m^3x^3+\quad bx^2+\quad cx+d.$$

And now, making $3m^2p=b$, or $p=\frac{b}{3m^2}$, there remains

$$cx+d=3mp^2x+p^3.$$

Whence

$$x=\frac{p^3-d}{c-3mp^2}.$$

Or, substituting for p its equivalent $\frac{b}{3m^2}$, we have

$$x=\frac{b^3-27dm^6}{(3cm^3-b^2)9m^3}.$$

Ex. 3. Required the value of x in the equation

$$x^3-3x^2+x=z^3.$$

Here $m=1$, $b=-3$, $c=1$, and $d=0$; therefore

$$x=\frac{b^3-27dm^6}{(3cm^3-b^2)9m^3}=\frac{1}{3},$$

which fraction gives $z^3=(\frac{1}{2})^3$, as required.

Ex. 4. Required the value of x in the equation

$$x^3+x-7=z^3.$$

Here $m=1$, $b=0$, $c=1$, and $d=-7$; therefore,

$$x=\frac{b^3-27dm^6}{(3cm^3-b^2)9m^3}=7,$$

which is the value of x required.

194. Case 3. *To find the value of x in the indeterminate equation*

$$m^3x^3+bx^2+cx+f^3=z^3.$$

Under this form the equation belongs to each of the foregoing cases, and may therefore be solved by either of them; it also admits of another solution on the following principles:

Assume

$$z=mx+f,$$

then, by cubing, we have

$$m^3x^3+3m^2fx^2+3mf^2x+f^3,$$
$$m^3x^3+\quad bx^2+\quad cx\ +f^3.$$

Whence,

$$bx^2+cx=3m^2fx^2+3mf^2x, \text{ or}$$
$$x=\frac{3mf^2-c}{b-3m^2f}.$$

We have, therefore, for indeterminate equations of this form, the following distinct solutions; *viz.*

$$\text{By case 1, } x=\frac{(c^2-3bf^3)9f^3}{27m^3f^6-c^3}.$$

$$\text{By case 2, } x=\frac{b^3-27f^3m^6}{(3cm^3-b^2)9m^3}.$$

$$\text{By case 3, } x=\frac{3mf^2-c}{b-3m^2f}.$$

That is, by writing m^3 for a, in case 1, and f^3 for d, in case 2.

Ex. 5. Find three values of x in the equation

$$x^3-3x^2+1=z^3.$$

Here $m=1$, $b=-3$, $c=0$, $f=1$; whence the three values of x, as determined by the above formulæ, are $x=3$, $x=\frac{2}{3}$, and $x=\frac{-1}{2}$.

Ex. 6. Required the values of x in the equation

$$x^3-3x-1=z^3.$$

Since $m=1$, $b=0$, $c=-3$, $f=-1$; therefore, the required values of x are, $x=\frac{-3}{2}$, $x=\frac{-1}{3}$, and $x=2$.

Remark. The above are the only cases in which the proposed equation admits of a direct solution, and even these all fail when b and c are both zero at the same time; that is, in equations of the form

$$ax^3+d=z^3,$$

which are, in fact, frequently impossible, as we have seen in Part I. chap. v. But if in any proposed equation of this kind one solution is known, others may be deduced from the known case, according to the following proposition.

PROP. VI.

195. Having given the values of m in the equation

$$am^3+bm^2+cm+d=f^3,$$

to find the values of x in the indeterminate equation

$$ax^3+bx^2+cx+d=z^3.$$

Assume

$$y+m=x;$$

then we have

$$\begin{aligned}
ay^3+3amy^2+3am^2y+am^3&=ax^3,\\
by^2+2bmy+bm^2&=bx^2,\\
cy+cm&=cx,\\
d&=d.
\end{aligned}$$

And now, writing

$$\begin{aligned} a \quad - \; - \; - \; - \; - \; - \; - \quad &= a', \\ 3am + b \quad - \; - \; - \; - \; - \; - \quad &= b', \\ 3am^2 + 2bm + c \quad - \; - \; - \quad &= c', \\ am^3 + bm^2 + cm + d \quad - \quad &= f^3, \end{aligned}$$

we have

$$\begin{aligned} a\,x^3 + b\,x^2 + c\,x + d &= z^3, \text{ or} \\ a'y^3 + b'y^2 + c'y + f^3 &= z^3; \end{aligned}$$

which last equation being of the form of that in the first case of the preceding proposition, we have

$$y = \frac{(c^2 - 3bf^3)9f^3}{27af^6 - c^3};$$

and, consequently, since $x = y + m$, the value of this quantity will also become known.

Ex. 1. Having given $m = 1$ in the equation

$$2m^3 - 1 = f^3,$$

it is required to find the values of x in the equation

$$2x^3 - 1 = z^3.$$

Here, since

$$2m^3 - 1 = 1^3,$$

we have $m = 1$, $f = 1$, $a = 2$, $b = 0$, $c = 0$, $d = -1$; therefore, $a' = 2$, $b' = 6$, $c' = 6$, and $f = 1$.

Whence

$$y = \frac{(c'^2 - 3b'f^3)9f^3}{27a'f^6 - c'^3} = -1,$$

so that $x = y + m = -1 + 1 = 0$, or $x = 0$; that is, we cannot find a second value of the indeterminate equation: and this is no imperfection in the rule, for the proposed equation is impossible, except in the particular case of $m = 1$, as may be readily demonstrated by the principles contained in art. 69.

Ex. 2. Required the value of x in the equation

$$x^2+x+1=z^3,$$

the known case being $m=-1$.

Here $a=0$, $b=1$, $c=1$, $d=1$; and, therefore, by the foregoing formula, we have $a'=0$, $b'=1$, $c'=-1$, and $f=1$; whence

$$y=\frac{(c'^2-3b'f^3)9f^3}{27a'f^6-c'^3}=\frac{-18}{+\ 1}=-18;$$

whence $x=-18-1=-19$, which number will be found to answer the required conditions for

$$19^2-19+1=7^3.$$

We shall here conclude our investigations with regard to those indeterminate equations in which there enters only one unknown quantity, and proceed to those in which two or more indeterminates are concerned, which, notwithstanding their apparent difficulty, frequently admit of general solutions, as will be seen in the following propositions.

PROP. VII.

196. To find the general values of x and y in the equation

$$x^2+axy+by^2=z^3.$$

We have demonstrated (art. 100), that if m and n are the two roots of the quadratic equation

$$\phi^2-a\phi+b=0,$$

the product of the two formulæ $(x+my)$ and $(x+ny)$, will be equal to

$$x^2+axy+by^2;$$

or, writing t for x, and u for y, we have

$$(t+mu)\times(t+nu)=t^2+atu+bu^2.$$

It also follows from art. 101 (retaining t and u instead of x and y), that the product of any number of factors of the form $t+mu$ is also of the same form; thus

$$(t+mu)(t'+mu')=\text{T}+m\text{U},$$

by making $\text{T}=tt'-buu'$, and $\text{U}=tu'+t'u+auu'$; and, in the same manner, we have

$$(\text{T}+m\text{U})(t''+mu'')=\text{T}'+m\text{U}',$$

where $\text{T}'=\text{T}t''-b\text{U}u''$, and $\text{U}'=\text{T}u''+t''\text{U}+a\text{U}u''$; whence again,

$$(t+mu)(t'+mu')(t''+mu'')=\text{T}'+m\text{U}', \text{ and}$$
$$(t+nu)\,(t'+nu')\,(t''+nu'')\;=\text{T}'+n\text{U}':$$

and, therefore, the continued product of these six factors gives

$$(\text{T}'+m\text{U}')(\text{T}'+n\text{U}')=\text{T}'^2+a\text{T}'\text{U}'+b\text{U}'^2.$$

Now if in the above six factors we make

$$t=t'=t'', \text{ and } u=u'=u'',$$

our product will become

$$(t+mu)^3(t+nu)^3=\text{T}'^2+a\text{T}'\text{U}'+b\text{U}'^2, \text{ or}$$
$$(t^2+atu+bu^2)^3\quad=\text{T}'^2+a\text{T}\,\text{U}'+b\text{U}^2;$$

that is, we shall have $\text{T}'^2+a\text{T}'\text{U}'+b\text{U}'^2$ a complete cube; and it only remains to find the values of T' and U in terms of t and u.

Now, for this purpose, we have

$$\text{T}=tt'-buu', \text{ and } \text{U}=tu'+t'u+auu';$$

or, since $t=t'=t''$, and $u=u'=u''$, these become

$$\text{T}=t^2-bu^2, \text{ and } \text{U}=2tu+au^2.$$

But we have again,

$$\text{T}'=\text{T}t''-b\text{U}u'', \text{ and } \text{U}'=\text{T}u''+t''\text{U}+a\text{U}u'';$$

and making $t''=t, u''=u$, and substituting the above value of T and U in this expression, we have

$$\text{T}' = t^3 - 3btu^2 - abu^3,$$
$$\text{U}' = 3t^2u + 3atu^2 + (a^2 - b)u^3.$$

Hence, then, we have the general solution of the equation

$$\text{T}'^2 + a\text{T}'\text{U}' + b\text{U}'^2 = z^3, \text{ or}$$
$$x^2 + axy + by^2 = z^2.$$

For we have only to assume

$$x = t^3 - 3btu^2 - abu^3,$$
$$y = 3t^2u + 3atu^2 + (a^2 - b)u^3;$$

and in these expressions we may give any values at pleasure to the indeterminates t and u, and we shall thus have

$$z^3 = (t^2 + atu + bu^2)^3.$$

Ex. 1. Required the values of x and y in the equation

$$x^2 + 3xy + 5y^2 = z^3.$$

By the above formulæ, we have $a = 3$ and $b = 5$, whence

$$x = t^3 - 15tu^2 - 15u^3,$$
$$y = 3t^2u + 9tu^2 + 4u^3.$$

And here, if we assume $t = 1$ and $u = 1$, we have $x = 1$ and $y = 16$; but if, in order to obtain a different value for x, we take $t = 5$ and $u = 1$, then the formulæ give $x = 35$ and $y = 124$, whence

$$x^2 + 3xy + 5y^2 = 45^3;$$

and it is obvious, that we may thus obtain an indefinite number of values of x and y, by only changing those of t and u.

Ex. 2. Required the values of x and y in the equation

$$x^2 - xy + 2y^2 = z^3.$$

Here we have $a=-1$ and $b=2$, so that the general values of x and y are

$$x=t^3-6tu^2+2u^3,$$
$$y=3t^2u-3tu^2-u^3.$$

And here, assuming $t=3$ and $u=1$, we have $x=11$ and $y=17$, whence

$$x^2-xy+2y^2=8^3.$$

Ex. 3. Find the values of x and y in the equation

$$x^2-7y^2=z^3.$$

Here we have $a=0$ and $b=-7$, whence the general expressions become

$$x=t^3+21tu^2,$$
$$y=3t^2u+7u^3.$$

Assuming now $t=3$ and $u=1$, we have $x=90$ and $y=34$, which gives

$$x^2-7y^2=2^3.$$

And an indefinite number of other values of x and y may be found, by changing the values of t and u.

PROP. VIII.

197. To find the general values of x and y in the equation

$$x^2+axy+by^2=z^4.$$

By the foregoing proposition, we have

$$(t+mu)^3=\text{T}'+m\text{U}', \text{ and}$$
$$(t+nu)^3=\text{T}'+n\text{U}'.$$

In which expressions we have

$$\text{T}'=t^3-3btu^2-abu^3,$$
$$\text{U}'=3t^2u+3atu^2+(a^2-b)u^3.$$

Now, from what has been before demonstrated,

$$(T' + mU')(t + mu) = T'' + mU'',$$
$$(T' + nU')(t + nu) = T'' + nU'',$$

in which we have

$$T'' = T't - bU'u, \text{ and } U'' = T'u + tU' + aU'u;$$

and since

$$(t + mu)^3 = T' + mU', \text{ and}$$
$$(t + nu)^3 = T' + nU',$$

we have

$$(T' + mU')(t + mu) = (t + mu)^4 = T'' + mU'',$$
$$(T' + nU')(t + nu) = (t + nu)^4 = T'' + nU''.$$

And hence (by art. 101) we obtain

$$(t + mu)^4 (t + nu)^4 = T''^2 + aT''U'' + bU''^2, \text{ or}$$
$$(t^2 + atu + bu^2)^4 = T''^2 + aT''U'' + bU''^2.$$

It therefore only remains to find the values of T'' and U'' in terms of t and u.

Now we have

$$T'' = T't - bU'u, \text{ and } U'' = T'u + tU' + aU'u; \text{ but}$$
$$T' = t^3 - 3btu^2 - abu^3, \text{ and}$$
$$U' = 3t^2u + 3atu^2 + (a^2 - b)u^3;$$

and substituting these values of T' and U' in the above expressions, we have

$$T'' = t^4 - 6bt^2u^2 - 4abtu^3 - (a^2b - b^2)u^4,$$
$$U'' = 4t^3u + 6at^2u^2 + 4(a^2 - b)tu^3 + (a^3 - 2ba)u^4.$$

Hence, then, we have the general solution of the equation,

$$T''^2 + aT''U'' + bU''^2, \text{ or } x^2 + axy + by^2 = z^4;$$

having only to assume for x and y, as above; *viz.*

$$x = t^4 - 6bt^2u^2 - 4abtu^3 - (a^2b - b^2)u^4,$$
$$y = 4t^3u + 6at^2u^2 + 4(a^2 - b)tu^3 + (a^3 - 2ba)u^4,$$

in which expressions we may give any values at pleasure to the indeterminates t and u, and we shall thus have

$$z^4 = (t^2 + atu + bu^2)^4.$$

Ex. Required the values of x and y in the equation

$$x^2 + 7y^2 = z^4.$$

Here we have $a = 0$ and $b = 7$, whence the general values of x and y will be

$$x = t^4 - 42t^2u^2 + 49u^4,$$
$$y = 4t^3u - 28tu^3.$$

And as it is indifferent whether x and y be negative or positive, we may assume $t = 1$ and $u = 1$; whence $x = 8$ and $y = 24$, which gives

$$x^2 + 7y^2 = 8^4.$$

And it is obvious how other values may be obtained by changing the values of t and u.

PROP. IX.

198. To find the general rational values of x and y in the equation

$$x^2 + axy + by^2 = z^k.$$

As the quantity $x^2 + axy + by^2$ is formed from the product of the two factors,

$$(x + my)(x + ny),$$

in order that it may become a power of the dimension k, each of its factors must be also complete powers of the same dimensions.

Let us therefore make

$$(x + my) = (t + mu)^k, \text{ and}$$
$$(x + ny) = (t + nu)^k.$$

From the development of the first of which expressions, we have, by writing 1, α, β, γ, δ, for the coefficients of the expanded binomial,

$$(t+mu)^k = x + my =$$
$$t^k + \alpha . t^{k-1}(mu) + \beta t^{k-2}(mu)^2 + \gamma t^{k-3}(mu)^3 + \&c.$$

Now, since m is one of the roots of the equation

$$\phi^2 - a\phi + b = 0,$$

we shall also have

$$m^2 - am + b = 0;$$

therefore,

$$m^2 = ma - b, \;\; m^3 = m^2 a - mb = (a^2 - b)m - ab,$$

because $a = (m+n)$, and $b = mn$, whence

$$(a^2 - b)m - ab = m^3;$$

and, in the same way, we find

$$m^4 = (a^2 - b)m^2 - mab =$$
$$(a^2 - 2ab)m - a^2 b + b^2;$$

and so on for the other powers of m.

We shall therefore only have to substitute these values in the preceding formula, and then we shall find that the expression will be compounded of two parts, one wholly rational, and the other a multiple of m; equating therefore the first with x, and the other with y, we shall obtain the general values of these quantities. And if, in order to simplify the result, we make

$$\begin{array}{ll} A' = 1, & B' = 0, \\ A'' = a, & B'' = b, \\ A''' = aA'' - bA', & B''' = aB'' - bB', \\ A^{iv} = aA''' - bA'', & B^{iv} = aB''' - bB'', \\ A^{v} = aA^{iv} - bA''', & B^{v} = aB^{iv} - bB''', \end{array}$$

we shall have

$$m = A' \, m - B',$$
$$m^2 = A'' \, m - B'',$$
$$m^3 = A''' m - B''',$$
$$m^4 = A^{iv} \, m - B^{iv},$$
$$\&c. \qquad \&c.$$

Therefore, substituting these values, and comparing, we shall have

$$\begin{cases} x = t^k - \alpha t^{k-1} u B' - \beta t^{k-2} u^2 B'' - \gamma t^{k-3} u^3 B''' - \\ \qquad \delta t^{k-4} u^4 B^{iv} - \&c. \end{cases}$$
$$\begin{cases} y = \alpha t^{k-1} u A' + \beta t^{k-2} u^2 A'' + \gamma t^{k-3} u^3 A''' + \\ \qquad \delta t^{k-4} u^4 A^{iv} + \&c. \end{cases}$$

$1, \alpha, \beta, \gamma$, &c., representing, as before, the coefficients of $(t+u)^k$.

And, as the root m does not enter into this expression, it is evident that, having

$$x + my = (t + mu)^k,$$

we shall likewise have

$$x + ny = (t + nu)^k;$$

and, consequently, multiplying these two equations together, we obtain

$$x^2 + axy + by^2 = (t^2 + atu + bu^2)^k;$$

and the values above found will be the general values of x and y in the equation

$$x^2 + axy + by^2 = z^k.$$

Cor. When the coefficient a, in the above formula, becomes zero, and the equation takes the form

$$x^2 + by^2 = z^k,$$

the above values of x and y become more simple, the alternate terms being destroyed; and we have then

$$x = t^k - \beta t^{k-2}u^2b + \delta t^{k-4}u^4b^2 - \varsigma t^{k-6}u^6b^3 - \&c.$$
$$y = \alpha t^{k-1}u - \gamma t^{k-3}u^3b + \varepsilon t^{k-5}u^5b^2 - \&c.$$

Ex. 1. Required the values of x and y in the equation

$$x^2 + 2xy + 3y^2 = z^5.$$

Here $a = 2$ and $b = 3$; therefore,

$$\begin{array}{llrllr}
\text{A}' = 1 & = & 1, & \text{B}' = 0 & = & 0, \\
\text{A}'' = a & = & 2, & \text{B}'' = b & = & 3, \\
\text{A}''' = a\text{A}'' - b\text{A}' & = & 1, & \text{B}''' = a\text{B}'' - b\text{B}' & = & 6, \\
\text{A}^{\text{iv}} = a\text{A}''' - b\text{A}'' & = & -4, & \text{B}^{\text{iv}} = a\text{B}''' - b\text{B}'' & = & 3, \\
\text{A}^{\text{v}} = a\text{A}^{\text{iv}} - b\text{A}''' & = & -11, & \text{B}^{\text{v}} = a\text{B}^{\text{iv}} - b\text{B}''' & = & -12.
\end{array}$$

Also the coefficients of $(t + u)^5$, being

$$1,\ 5,\ 10,\ 10,\ 5,\ 1,$$

we have $\alpha = 5$, $\beta = 10$, $\gamma = 10$, $\delta = 5$, $\varepsilon = 1$; whence the general values of x and y become

$$x = t^5 - 10.3t^3u^2 - 10.6t^2u^3 - 5.3tu^4 + 12u^5,$$
$$y = 5t^4u + 10.2t^3u^2 + 10.1t^2u^3 - 5.4tu^4 - 11u^5.$$

By assuming $t = 1$ and $u = 1$, we have $x = -92$ and $y = 4$; whence

$$x^2 + 2xy + 3y^2 = 6^5.$$

Ex. 2. Required the values of x and y in the equation

$$x^2 + y^2 = z^6.$$

Here $a = 0$, $b = 1$, $k = 6$; and, therefore, we have $\alpha = 6$, $\beta = 15$, $\gamma = 20$, $\delta = 15$, $\varepsilon = 6$, $\varsigma = 1$, for the coefficients of $(t + u)^6$.

Whence, by the foregoing corollary,

$$x = t^6 - 15t^4u^2 + 15t^2u^4 - u^6,$$
$$y = 6t^5 - 20t^3u^3 + 6tu^5.$$

Assuming here $t=2$ and $u=1$, we find $x=117$ and $y=44$, which gives

$$x^2+y^2=5^6,$$

as required. And other values may be found by changing those of t and u.

PROP. X.

199. To find the general values of x and y in the equation

$$x^3+ax^2y+bxy^2+cy^3=z^2.$$

This is one of the most difficult problems we have yet attempted, and is deserving of particular attention, not only on account of its difficulty, but because a general solution would be obtained with very great difficulty, if indeed it be at all possible to arrive at it by any other method.

Here we must consider the product of these three factors

$$(t+mu+m^2w)(t+nu+n^2w)(t+pu+p^2w),$$

m, n, and p, being the three roots of the cubic equation

$$\phi^3-a\phi^2+b\phi-c=0;$$

and, consequently,

$$m+n+p=a,\ mn+mp+np=b,\ \text{and}\ mnp=c.$$

Now by the real development of the above factors we obtain

$$\begin{aligned}&(t+mu+m^2w)(t+nu+n^2w)(t+pu+p^2w)=\\&\quad t^3+\\&\quad (m+n+p)t^2u+\\&\quad (m^2+n^2+p^2)t^2w+\\&\quad (mn+mp+np)tu^2+\end{aligned}$$

$$(m^2n + m^2p + n^2m + n^2p + p^2m + p^2n)tuw +$$
$$(m^2n^2 + m^2p^2 + n^2p^2)tw^2 +$$
$$(mnp)u^3 +$$
$$(m^2np + n^2mp + p^2mn)u^2w +$$
$$(m^2n^2p + m^2p^2n + n^2p^2m)uw^2 +$$
$$(m^2n^2p^2)w^3.$$

And, since

$m + n + p = a$, $mn + mp + np = b$, and $mnp = c$,

we shall find that

$$\begin{array}{ll}
1 \text{ - - - - - - - - -} & = 1, \\
(m + n + p) \text{ - - - - - - - -} & = a, \\
(m^2 + n^2 + p^2) \text{ - - - - - - -} & = a^2 - 2b, \\
(mn + mp + np) \text{ - - - - - -} & = b, \\
(m^2n + m^2p + n^2m + n^2p + p^2m + p^2n) & = ab - 3c, \\
(m^2n^2 + m^2p^2 + n^2p^2) \text{ - - - -} & = b^2 - 2ac, \\
(mnp) \text{ - - - - - - - -} & = c, \\
(m^2np + n^2mp + p^2mn) \text{ - - -} & = ac, \\
(m^2n^2p + m^2p^2n + n^2p^2m) \text{ - - -} & = bc, \\
(m^2n^2p^2) \text{ - - - - - - - -} & = c^2.
\end{array}$$

Therefore, making these substitutions, the product becomes

$$t^3 + at^2u + (a^2 - 2b)t^2w + btw^2 + (ab - 3c)tuw +$$
$$(b^2 - 2ac)tw^2 + cu^3 + acu^2w + bcuw^2 + c^2w^3.$$

But any two factors of the form

$$(t + mu + m^2w)(t' + mu' + m^2w'),$$

always produce a product having the same form as each of those factors; and, therefore, the above formula will have this property, that, if we multiply together as many similar formulæ as we please, the product will always have a similar form.

Suppose, for example, that it were required to multiply the above by a similar formula,

$t'^3 + at'^2u' + (a^2-2b)t'^2w' + bt'u'^2 + (ab-3c)t'u'w' + (b^2-2ac)t'w'^2 + cu'^3 + acu'^2w' + bcu'w'^2 + c^2w'^3$.

Since this last may be supposed to be generated from the multiplication of

$$(t'+mu'+m^2w')(t'+nu'+n^2w')(t'+pu'+p^2w),$$

we have only to seek the product of the six following factors,

$$\begin{cases} (t+mu+m^2w)(t+nu+n^2w)(t+pu+p^2w) \\ (t'+mu'+m^2w')(t'+nu'+n^2w')(t'+pu'+p^2w'): \end{cases}$$

and, first, let us take two of them; *viz.*

$$(t+mu+m^2w)(t'+mu'+m^2w),$$

the product of which is

$$\begin{cases} tt'+m(tu'+ut')+m^2(tw'+wt'+uu')+m^3(uw'+ \\ \quad wu')+m^4ww'. \end{cases}$$

Now, m being one of the roots of the equation

$$\phi^3 - a\phi^2 + b\phi - c = 0,$$

we have

$$m^3 - am^2 + bm - c = 0, \text{ or}$$
$$m^3 = am^2 - bm + c;$$

whence

$$m^4 = am^3 - bm^2 + mc = (a^2-b)m^2 - (ab-c)m + ac;$$

so that substituting these values, and, in order to simplify the result, making

$$\text{T} = tt' + c(uw'+wu') + acww',$$
$$\text{U} = tu' + ut' - b(uw'+wu') - (ab-c)ww',$$
$$\text{W} = tw' + wt' + uu' + a(uw'+wu') + (a^2-b)ww',$$

we shall have

$$(t+mu+m^2w)(t'+mu'+m^2w') = \text{T} + m\text{U} + m^2\text{W};$$

and, in the same manner, we obtain

$$(t+nu+n^2w)(t'+nu'+n^2w')=\text{T}+n\text{U}+n^2\text{W},$$
$$(t+pu+p^2w)(t'+pu'+p^2w')=\text{T}+p\text{U}+p^2\text{W}.$$

And, therefore, the product of the six foregoing formulæ is the same as that of the three,

$$(\text{T}+m\text{U}+m^2\text{W})(\text{T}+n\text{U}+n^2\text{W})(\text{T}+p\text{U}+p^2\text{W})=$$
$$\text{T}^3+a\text{T}^2\text{U}+(a^2-2b)\text{T}^2\text{W}+b\text{TU}^2+(ab-3c)\text{TUW}+$$
$$(b^2-2ac)\text{TW}^2+c\text{U}^3+ac\text{U}^2\text{W}+bc\text{UW}^2+c^2\text{W}^3.$$

Now, making $t=t'$, $u=u'$, $w=w'$, this last formula becomes equal to the product

$$(t+mu+m^2w)^2(t+nu+n^2w)^2(t+pu+p^2w)^2,$$

and is therefore a square, and the values of T, U, and W, before determined, now become

$$\text{T}=t^2+2cuw+acw^2,$$
$$\text{U}=2tu-2buw-(ab-c)w^2,$$
$$\text{W}=2tw+u^2+2auw+(a^2-b)w^2.$$

We have, therefore, the general solution of the equation above given; *viz.*

$$\text{T}^3+a\text{T}^2\text{U}+(a^2-2b)\text{T}^2\text{W}+b\text{TU}^2+(ab-3c)\text{TUW}+$$
$$(b^2-2ac)\text{TW}^2+c\text{U}^3+ac\text{U}^2\text{W}+bc\text{UW}^2+c^2\text{W}^3=z^2.$$

But in order to make this apply to our equation

$$x^3+ax^2y+bxy^2+cy^3=z^2,$$

we must take $x=\text{T}$, $y=\text{U}$, and $0=\text{W}$, which reduces it precisely to our case.

Therefore, when it is required to find rational values of x and y in the equation

$$x^3+ax^2y+bxy^2+cy^3=z^2,$$

we must have, first,

$$2tw+u^2+2auw+(a^2-b)w^2=0;\ \text{or}$$

$$t=-\frac{u^2+2auw+(a^2-b)w^2}{2w}.$$

Then we obtain, by writing x and y for T and U,

$$\begin{cases} x = t^2 + 2cuw + acw^2, \\ y = 2tu - 2buw - (ab - c)w^2, \end{cases}$$

in which expressions u and w may be assumed at pleasure, but the value of t will depend upon the equation

$$t = -\frac{u^2 + 2auw + (a^2 - b)w^2}{2w}.$$

Cor. When any of the coefficients a, b, or c, become zero, the result is much simplified; thus, if $a = 0$ and $b = 0$, or the equation takes the form

$$x^3 + cy^3 = z^2,$$

then the values of x and y will be expressed by the formulæ

$$t = -\frac{u^2}{2w}, \text{ and}$$

$$\begin{cases} x = t^2 + 2cuw, \\ y = 2tu + cw^2; \end{cases}$$

or, by substituting for w, we have

$$x = t^2 - \frac{cu^3}{t},$$

$$y = 2tu + \frac{cu^4}{4t^2}; \text{ or}$$

$$\begin{cases} x = 4t^4 - 4cu^3t, \\ y = 8t^3u + cu^4; \end{cases}$$

the last formulæ being found by reducing the two first to the common denominator $4t^2$, and then rejecting it in both the values of x and y.

Ex. 1. Required the values of x and y in the equation

$$x^3 + y^3 = z^2.$$

Here we have $c=1$, and therefore the values of x and y are expressed by the formulæ

$$\begin{cases} x=4t^4-4u^3t, \\ y=8t^2u+u4, \end{cases}$$

where t and u may be assumed at pleasure; if we take $t=1$ and $u=-3$, we have $x=112$ and $y=57$, which gives

$$x^3+y^3=z^2, \text{ or } 112^3+57^3=1261^2;$$

and other values of x and y may be found by changing those of t and u.

Ex. 2. Required the values of x and y in the equation

$$x^3-3y^3=z^2.$$

Here $c=-3$; and, therefore, the general values of x and y may be represented by the formulæ

$$\begin{cases} x=4t^4+12u^3t, \\ y=8t^3u-3u^4; \end{cases}$$

where, by taking $t=2$ and $u=1$, we have $x=88$ and $y=61$, which give

$$88^3-3.61^3=23^2;$$

and if we had taken $t=1$ and $u=1$, we should have had $t=16$ and $y=5$, whence

$$16^3-3.5^3=61^2;$$

and an infinite number of other values may be found for x and y, by changing those of t and u.

Ex. 3. Find the values of x and y in the equation

$$x^3+5y^3=z^2.$$

Here $c=5$, and hence the general values of x and y are

$$\begin{cases} x=4t^4-20u^3t, \\ y=8t^3u+5u^4; \end{cases}$$

by taking $t=2$ and $u=1$, we have $x=24$ and $y=69$, whence

$$24^3+5.69^3=1287^2;$$

and, by changing the values of t and u, an infinite number of integral values may be found for x and y.

Ex. 4. Find the values of x and y in the equation

$$x^3+2x^2y+2xy^2+y^3=z^2.$$

Here we must have recourse to our first values of x and y; *viz.*

$$t=-\frac{u^2+2auw+(a^2-b)w^2}{2w},$$

$$\begin{cases} x=t^2+2cuw+acw^2, \\ y=2tu-2buw-(ab-c)w^2. \end{cases}$$

In which expressions we have $a=2$, $b=2$, $c=1$, and u and w indeterminates that may be assumed at pleasure; by taking $u=1$ and $w=1$ we have

$$t=-\frac{1+4+2}{2}=-\frac{7}{2},$$

$$x=\frac{49}{4}+2+2=\frac{65}{4},$$

$$y=7-4-3=-14;$$

which values of x and y answer the required conditions of the equation, as will also the integers

$$x=65 \text{ and } y=-56.$$

Practical Examples.

1. Required the value of x in the equation

$$x^3+3=z^2.$$

Ans. $x=\frac{-23}{16}$, or $\frac{1873}{1521}$.

2. Required the value of x in the equation

$$3x^3+1=z^2.$$

Ans. $x=\frac{-5}{16}$, or $\frac{8}{25}$, or $\frac{-629}{1323}$.

3. Required the value of x in the equation

$$2x^4-3x^2+2=z^2, \text{ and } x^4-x^2+1=z^2,$$

or prove that such values cannot be found, except in the obvious case of

$$x=\pm 1.$$

Ans. Impossible.

4. To ascertain the values of x in the equation

$$x^4+8x^2+1=z^2.$$

Ans. $x=2$, or $\frac{15}{28}$, or $\frac{58}{2911}$.

5. Required the values of x in the equation

$$x^2+2=z^3.$$

Ans. $x=5$, or $\frac{383}{1000}$.

6. Required the possibility or impossibility of the equation

$$x^3+1=z^2,$$

except in the known case of $x=2$.

Ans. Impossible.

7. To find the values of x in the equation

$$3x^3+3=z^3.$$

Ans. $x=2$, or $\frac{-20}{17}$.

8. Required the values of x in the equation

$$x^2+4=z^3.$$

Ans. $x=11$, or $\frac{-1090}{27}$.

9. To find the value of x in the equation

$$x^2+7=z^4.$$

Ans. $x=\frac{367}{144}$.

10. Required the integral value of x and y in the equation

$$x^2+7xy+5y^2=z^2.$$

11. To find the integral values of x and y in the equation

$$x^2+7y^2=z^3.$$

12. Required rational and integral values of x and y in the equation

$$x^3+7y^3=z^2.$$

13. Find integral values of x and y in the equation

$$2x^2-7y^2=16z^5.$$

CHAP. V.

On the Solution of Indeterminate Equations of the Form $x^n - b = \text{M}(a)$. Or the Method of determining x, such that $x^n - b$ may be divisible by a.

PROP. I.

200. To ascertain the possibility or impossibility of every equation of the form

$$x^n - b = \text{M}(a),$$

and the number of solutions in the former case, a being a prime number.

First it is obvious, that, if $b = a$, or any multiple of a, the equation admits of an infinite number of solutions, by assuming $x = a$, or any multiple of a; we shall therefore only consider those cases in which b is prime to a.

Let, then, b be prime to a; and suppose, first, that n and $a-1$ have a common measure w; that is, suppose $n = n'w$, and $a - 1 = a'w$; then I say, that, if the equation admits of one solution, it will also admit of w solutions, and no more.

For, if the equation be possible, we shall have

$$x^{n'w} - b = \text{M}(a).$$

But, since a is a prime number,

$$x^{a'w} - 1 = \text{M}(a) \quad \text{(art. 87)}.$$

And now, if by art. 159 we find two other numbers, p and q, such that

$$n'p - a'q = 1, \text{ or } n'p = a'q + 1,$$

we shall have, by means of this and the foregoing equations, which, by rejecting the multiples of a, may be written thus,

$$x^{n'w} \doteqdot {}^{*}b, \text{ and } x^{a'w} \doteqdot 1,$$

the following results; *viz.*

$$b^p \doteqdot x^{pn'w} \doteqdot x^{qa'w+w} \doteqdot x^w, \text{ or } x^w \doteqdot b^p;$$

whence

$$x^w - b^p = \text{M}(a).$$

Therefore, when the equation is solvible, x must have such a value that x^w, when divided by a, shall leave the same remainder as b^p divided by a; but (by cor., art. 87) the equation

$$x^w - c = \text{M}(a),$$

will have w different solutions, and no more; and, consequently, when the proposed equation is possible, it will have also w solutions, and no more.

Now, with regard to the possibility of the equation, it will depend upon that of

$$b^{\frac{a-1}{w}} - 1 = \text{M}(a);$$

that is, if $b^{\frac{a-1}{w}} - 1$ be divisible a, the proposed equation will be possible, but otherwise it will not.

For, since $x^{n'w} \doteqdot b$ and $x^{a'w} \doteqdot 1$, we have

$$b^{a'} \doteqdot x^{n'a'w} \doteqdot 1^{n'} \doteqdot 1, \text{ or } b^{a'} \doteqdot 1;$$

* This character indicates, that $x^{n'w}$ is of the same form as b to modulus a, or that their remainders are equal when divided by a.

but $a-1=a'w$, therefore $a'=\frac{a-1}{w}$; and, consequently, $b^{\frac{a-1}{w}} \doteq 1$, or

$$b^{\frac{a-1}{w}}-1=\text{M}(a),$$

which equation must necessarily have place when the proposed equation is possible; and, therefore, by means of this, the possibility or impossibility of the proposed equation may be readily ascertained; and, in the former case, the number of its solutions will be w, as we have seen above, the whole of which are contained in the equation

$$x^w-b^p=\text{M}(a).$$

And it is obvious that, when one of these solutions is obtained, the others will be found by multiplying the known root by each of the roots of the equation

$$x^n-1=\text{M}(a);$$

for if r^n divided by a leave a remainder b, and r'^n divided by a leave a remainder 1, then will $r^nr'^n$ divided by a, also leave a remainder b; therefore, if r be one root of the equation

$$x^n-b=\text{M}(a),$$

and r', r'', r''', &c., be roots of the equation

$$x^n-1=\text{M}(a),$$

the other roots of the first equation will be

$$r,\ rr',\ rr'',\ rr''',\ \&\text{c}.$$

We shall, therefore, after illustrating what has been taught by two examples, proceed to the solution of this last equation.

Cor. 1. If $n>a-1$, we need only consider the

remainder arising from the division of n by $a-1$. For since

$$x^{a-1} - 1 = \text{M}(a) \text{ (art. 87)},$$

or, according to our contracted notation, $x^{a-1} \doteqdot 1$, we shall have

$$x^{m(a-1)+n} \doteqdot x^n;$$

that is, $x^{m(a-1)+n}$ will leave the same remainder as x^n, when both are divided by a.

Cor. 2. It follows also from the above proposition, that when n is prime to $a-1$ the equation is always possible. For in this case $w = 1$, and, therefore, $x \doteqdot b^p$, the exponent p being deduced from the equation

$$pn - q(a-1) = 1.$$

Ex. 1. It is required to ascertain whether the equation

$$x^7 - 11 = \text{M}(29)$$

be possible in integers.

By the above proposition, if this equation be possible, so also must

$$b^{\frac{a-1}{w}} - 1 = \text{M}(a).$$

Now, in this case, $a = 29$, $b = 11$, and $w = 7$; and, therefore, this last becomes

$$11^4 - 1 = \text{M}(29);$$

which equation being impossible, the proposed equation is impossible also.

Ex. 2. Required the number of possible solutions that may be given to the equation

$$x^6 - 2 = \text{M}(31).$$

Here $a=31$, $b=2$, and $w=6$; and since we have

$$2^{\frac{31-1}{6}}-1=\text{M}(31),$$

the equation is possible, and admits of six solutions.

PROP. II.

201. To find all the values of x in the indeterminate equation

$$x^n-1=\text{M}(a),$$

a being itself a prime number.

Case 1. *When n is prime to $a-1$.*

Here we shall have (by art. 87, and by writing r instead of x) $r^{a-1}-1=\text{M}(a)$; and, consequently,

$$r^{(a-1)n}-1=\text{M}(a), \text{ or } (r^{a-1})^n-1=\text{M}(a);$$

and, therefore,

$$(r^{a-1})^n=x^n, \text{ or } x=r^{a-1}=1;$$

that is, $x=1$, which is the only possible solution in this case.

Case 2. *Let n be a divisor of $a-1$.*

Since we may here make $a-1=a'n$, we shall have (by art. 87)

$$r^{a'n}-1=\text{M}(a);$$

and, consequently,

$$r^{a'n}=x^n, \text{ or } x=r^{a'},$$

where r may be assumed any number whatever prime to a.

If now we make $r^{a'}\doteq r'$, r' being the remainder arising from the division of $r^{a'}$ by a, then, since

$$r'^n-1=\text{M}(a),$$

we have also

$$r'^{mn}-1=\text{M}(a);$$

therefore, if r' be one root, r'^m will be another, whatever value we give to m, and since the equation

$$r'^n - 1 = \text{M}(a),$$

can have but n solutions, or roots, these will be found, either wholly or in part, in the series,

$$r',\ r'^2,\ r'^3,\ r'^4,\ \&c.\ r'^{n-1};$$

that is, this series, or the remainder of each term when divided by a, will furnish all the roots of the proposed equation, if these remainders be all different from each other, but they will give only a part of the n roots, if any two or more of them leave the same remainder.

Remark. When the root r' is such that the terms of the above series leave different remainders, then r' is said to be a *primitive root* of the equation

$$x^n - 1 = \text{M}(a);$$

and as we shall have frequent occasion to employ these quantities in chapter vii., it will not be amiss to demonstrate here some of the principal properties of these roots, after which we will give a few examples by way of illustration.

PROP. III.

202. If r be a root of the indeterminate equation

$$x^n - 1 = \text{M}(a),$$

$x^n - 1 = M$

and such that $r^{\frac{n}{m}} - 1$ be not divisible by a (m being any divisor of n), then I say, r is a primitive root; or, which is the same, all the roots of the above equation will be contained in the series

$$r, \; r^2, \; r^3, \; r^4, \; \&c. \; r^{n-1};$$

or the remainders of these, when divided by a, will be all different from each other.

For, if possible, let any two terms of this series give equal remainders, and let them be denoted by r^p and r^q, then it is obvious that we shall have

$$r^p - r^q = \text{M}(a), \text{ or}$$
$$r^{p-q} - 1 = \text{M}(a);$$

or, making $p-q=s$, it becomes

$$r^s - 1 = \text{M}(a):$$

and let the common divisor of n and s be k, which will be unity, when n and s are prime to each other; and if now, as in art. 200, we resolve the equation

$$np' - sq' = k, \text{ or } np' = sq' + k,$$

we shall, as in that article, have this result,

$$r^{np'} \doteqdot r^{sq'+k};$$

and since, by hypothesis,

$$r^n - 1 = \text{M}(a), \text{ and } r^s - 1 = \text{M}(a),$$

we shall have, by rejecting the multiples of a, $r^n \doteqdot 1$; therefore,

$$r^{np'} \doteqdot r^{sq'+k} \doteqdot r^k \doteqdot 1;$$

that is,

$$r^k - 1 = \text{M}(a).$$

Now, since $s=p-q$ must necessarily be less than n, and since k is the common divisor of s and n, we may make $n=mk$, or $\frac{n}{m}=k$, and $s=s'k$; and, consequently,

$$r^{\frac{n}{m}} - 1 = \text{M}(a),$$

which is contrary to what we have supposed; therefore, no two of the terms in the series

$$r,\ r^2,\ r^3,\ r^4,\ \&\text{c. } r^{n-1},$$

can leave the same remainder, and, consequently, r is in this case a primitive root of the proposed equation; and, therefore, all its n roots will be found in the above series.

Cor. It follows from this demonstration, that, if n be a prime number, every root r, of the equation

$$x^n - 1 = \text{M}(a),$$

is a primitive root, and will give, by its successive powers, all the roots of the proposed equation.

Thus, for example, since

$$3^5 - 1 = \text{M}(11),$$

we shall have also $9^5 - 1$, $5^5 - 1$, $4^5 - 1$, each divisible by 11; or, which is the same,

$$3,\ 3^2,\ 3^3,\ 3^4,$$

or their remainders when divided by 11; *viz.*

$$3,\ 9,\ 5,\ 4,$$

for the roots of the equation

$$x^5 - 1 = \text{M}(11).$$

PROP. IV.

203. If m, p, q, &c. be different prime divisors of n, then will the number of primitive roots of the equation

$$x^n - 1 = \text{M}(a)$$

be expressed by the following formula,

$$n \times \frac{m-1}{m} \times \frac{p-1}{p} \times \frac{q-1}{q},\ \&\text{c.}$$

For (by cor., art. 88) there are only n values of x, that satisfy the equation

$$x^n - 1 = \text{M}(a);$$

and there must also, by the same article, be $\frac{n}{m}$ values only that fulfil the condition of the equation

$$x^{\frac{n}{m}} - 1 = \text{M}(a);$$

and, consequently, out of the n first roots, there are $n - \frac{n}{m}$, that will not answer the last condition; and, in the same manner, we find there are $n - \frac{n}{p}$ that will not fulfil the conditions of the equation

$$x^{\frac{n}{p}} - 1 = \text{M}(a);$$

and proceeding thus with all the factors of n, we ascertain, finally, from the same principles as those employed at art. 24, that the whole number of primitive roots is expressed by the formula

$$n \times \frac{m-1}{m} \times \frac{p-1}{p} \times \frac{q-1}{q}, \text{ \&c.}$$

Q. E. D.

Cor. 1. If n be a prime number, every number that is prime to a is a primitive root.

Cor. 2. If n be any power of a prime number, as $n = m^r$, we must assume such a root r for x, that the equation

$$r^{\frac{n}{m}} - 1 = \text{M}(a)$$

has not place, then will the successive powers of r be the roots sought.

Cor. 3. If n be of the form $m^{\alpha} p^{\beta} q^{\gamma}$, we may

make $m^{\alpha} = \mu$, $p^{\beta} = \mu'$, $q^{\gamma} = \mu''$, by rejecting the multiples of a, if these quantities are $> a$, and then resolve the separate equations

$$x^{\mu} - 1 = \text{M}(a),\ x^{\mu'} - 1 = \text{M}(a),\ x^{\mu''} - 1 = \text{M}(a).$$

Now supposing the roots of these equations to be

$$r,\ r',\ r'',$$

the root of the proposed equation will be $rr'r''$; and the other roots will be the successive powers of this last quantity.

Ex. 1. Required the seven values of x in the equation

$$x^7 - 1 = \text{M}(379).$$

Since $379 - 1 = 7 . 54$ we have $x = r^{54}$, where r may be any number prime to 379 (art. 201).

Assume, therefore, $r = 2$, and we have, by rejecting successively the multiples of 379,

$$r^6 \doteqdot 64,\ r^{12} \doteqdot 306,\ r^{24} \doteqdot 23,\ r^{48} \doteqdot 150,\ r^{54} \doteqdot 125.$$

Therefore, $x = 125$; and since the power 7 is a prime number, this root is a primitive root, and gives, by its successive powers, or by their remainders, all the seven roots of the proposed equation; that is,

$$x = 125,\ 125^2,\ 125^3,\ 125^4,\ 125^5,\ 125^6,\ 125^7; \text{ or}$$
$$x = 125,\ 86,\ 138,\ 195,\ 119,\ 94,\ 1;$$

which last are the seven roots required.

Ex. 2. It is required to find the values of x in the equation

$$x^{63} - 1 = \text{M}(379).$$

Since $63 = 7 . 9$ we may (cor. 3, above) resolve the two equations

$$x^7 - 1 = \text{M}(379), \text{ and } x^9 - 1 = \text{M}(379);$$

the roots of the first being $r = 125$, and of the second $r' = 180$; and the product of these, rejecting the multiples of 379, is 139, which is one of the roots of the proposed equation, the others being contained in the series

$$139, \ 139^2, \ 139^3, \ 139^4, \ \&c. \ 139^9.$$

PROP. V.

204. To find the value of x in the indeterminate equation

$$x^{2n} + 1 = \text{M}(a),$$

a being a prime number, and $4n$ a divisor of $a - 1$.

Find the general value of x in the equation

$$x^{4n} - 1 = \text{M}(a)$$

by the foregoing propositions, and let this general root be represented by r^m, then will r^{2p+1} be the general root of the proposed equation

$$x^{2n} + 1 = \text{M}(a),$$

where p may be taken any number whatever.

For, r^m being any root of the equation

$$x^{4n} - 1 = \text{M}(a),$$

it follows, that r^{2m} is a root of the equation

$$x^{2n} - 1;$$

because r^m, being substituted for x in

$$x^{4n} - 1 = \text{M}(a),$$

is the same as r^{2m}, substituted for x in the equation

$$x^{2n} - 1 = \text{M}(a).$$

Now

$$x^{4n} - 1 = (x^{2n} - 1)(x^{2n} + 1);$$

and since the first of these factors has for its roots

all the even powers of r, there remain all the odd powers of r for the roots of the other factor, which is the equation proposed.

Ex. Required the values of x in the equation

$$x^{36} + 1 = \text{M}(433).$$

First, the solution of the equation

$$x^{72} - 1 = \text{M}(433),$$

by proposition 2, gives $x = r^6$, because

$$433 - 1 = 432 = 72 \times 6.$$

And by assuming $r = 5$, we have $5^6 = 37$, rejecting as before the multiples of 433; and, therefore,

$$37^{2p+1} = x,$$

is the general root in the proposed equation, which, by assuming $p = 0, 1, 2, 3,$ &c., and rejecting the multiples of 433, we have the following solution:

$$x = \begin{cases} \pm 37,\ 8,\ 127,\ 203,\ 79,\ 99,\ 2,\ 140,\ 159, \\ \quad 128,\ 133,\ 216,\ 35,\ 148,\ 32,\ 75,\ 54,\ 117, \end{cases}$$

the sign $\pm$ being common to each of the roots.

PROP. VI.

205. To find the values of x in the equation

$$x^n - b = \text{M}(a),$$

b being such that $b^m \pm 1$ is divisible by a, and m a divisor of $\frac{a-1}{n}$.

This proposition divides itself into two cases, *viz.* first when n and m are prime to each other, and second, when these quantities have a common measure.

Case 1. *When n and m are prime to each other.*

Find two other quantities, p and q, such that

$$pn - qm = 1, \text{ or } pn = qm + 1;$$

then will $x = b^p y$ be one root of the equation sought, y being itself a root of the equation

$$y^n - (\pm 1)^q = \text{M}(\text{A}).$$

For, by making $x = b^r y$, we have

$$x^n \doteqdot b^{pn} y^n \doteqdot b^{qm+1} y^n \doteqdot b y^n \doteqdot b;$$

and, consequently,

$$x^n - b = \text{M}(a).$$

Case 2. *When n and m have any common divisor w.*

Let $n = n'w$, and find the values of p and q, such that

$$pn' - qm = 1, \text{ or } pn' = qm + 1;$$

then we shall have $x^w = b^p y$, or

$$x^w - b^p y = \text{M}(a),$$

y being one of the roots of the equation

$$y^{n'} - (\pm 1)^q = \text{M}(a).$$

For, by making here $x^w = b^r y$, we have

$$x^{wn'} \doteqdot b^{pn'} y^{n'} \doteqdot b^{qm+1} y^{n'} \doteqdot b y^{n'} \doteqdot b;$$

and, consequently,

$$x^n - b = \text{M}(a).$$

Remark. By means of the above proposition, we are enabled to convert a number of equations, such as

$$x^n - b = \text{M}(a)$$

into others of the form

$$x^n \pm 1 = \text{M}(a).$$

It furnishes us also with the means of resolving, in an infinite number of the cases, the equation

$$x^n - b = \text{M}(a),$$

into n' equations of an inferior degree, as will appear from the following examples.

Ex. 1. Required the values of x in the equation

$$x^3 + 49 = \text{M}(223).$$

First, since $223 - 1 = 3 . 74$, and

$$(-49)^{74} - 1 = \text{M}(223),$$

the proposed equation is possible (art. 200); which fact being ascertained, we have $m = 74$, and it now remains to find

$$3p - 74q = 1, \text{ or } 3p = 74q + 1,$$

which equation gives $p = 25$.

Whence

$$x = (-49)^{25} y,$$

y being a root of the equation

$$y^3 - 1 = \text{M}(223),$$

the general form of which (by art. 201) is $y = r^{74}$, where r may be assumed at pleasure; and, therefore, the required root x, of the proposed equation, is

$$x = (-49)^{25} . r^{74},$$

the remainders of which, when divided by 223, will be the simplest form of the root sought: thus we find the required roots are

$$x = -36, \ -66, \ +102.$$

Remark. We should have obtained this solution more readily by first solving the equation

$$x^3 + 7 = \text{M}(223),$$

the three roots of which, squared, would have furnished the roots of the equation proposed.

And this method may be employed in all cases

in which b is a complete power; for, generally, if r be any root of the equation

$$x^n - b = \text{M}(a),$$

we have r^k for a root of the equation

$$x^n - b^k = \text{M}(a).$$

Ex. 2. Required the value of x in the equation

$$x^6 + 20 = \text{M}(61).$$

First, since $61 - 1 = 6 . 10$, and $b = -20$, we have

$$(-20)^{10} - 1 = \text{M}(61), \text{ or } (-20)^5 + 1 = \text{M}(61);$$

therefore the proposed equation is possible (art. 200); and since this last exponent 5, or (m), is prime to that proposed 6, or (n), it follows, from the first case of the preceding proposition, that $x = b^p y$, p being first found from the equation

$$6p - 5q = 1, \text{ or } 6p = 5q + 1,$$

and y from the equation

$$y^n + 1^q = \text{M}(61);$$

therefore $p = 1$ and $q = 1$; also (by art. 204) the general root of y is 29^{2k+1}; and, consequently, the general value of x, in the proposed equation, is

$$x = -20 . 29^{2k+1},$$

which, by involving and dividing, gives

$$x = \pm 7, \ \pm 24, \ \pm 30.$$

Ex. 3. To find the values of x in the equation

$$x^{10} - 5 = \text{M}(601).$$

Here we find

$$b^6 + 1 = \text{M}(601),$$

and since 10 and 6 have a common measure 2, we shall have, by the second part of the above proposition,

$$x^2 = b^5 y, \text{ or } x^2 - b^5 y = \text{M}(601),$$

y being a root of the equation

$$y^5 - 1 = \text{M}(601),$$

the general root of which is $y = (-169)^k$; and thus the proposed equation may be transformed into the five following ones of the second degree; *viz.*

$$x^2 - 120 = \text{M}(601),\ x^2 - 154 = \text{M}(601),$$
$$x^2 - 276 = \text{M}(601),\ x^2 - 234 = \text{M}(601),$$
$$x^2 + 183 = \text{M}(601).$$

PROP. VII.

206. To find the value of x in the equation

$$x^n - b = \text{M}(a);$$

in which

$$b^w - 1 = \text{M}(a);$$

w being a divisor of $\dfrac{a-1}{n}$.

Let $x = r^m$ be the general root of the equation

$$x^{nw} - 1 = \text{M}(a),$$

now, since b is found in the series

$$r^n,\ r^{2n},\ r^{3n},\ r^{4n},\ \&\text{c.},\ r^{(w-1)n};$$

let the term in which it is contained be $r^{\mu n}$, then will the general root of the proposed equation be

$$x = r^{w+m\mu}.$$

For, since $r^{mw+\mu} = x$, we have

$$x^n = r^{nmw+n\mu} = r^{n\mu} = b;$$

and, consequently,

$$x^n - b = \text{M}(a).$$

It therefore only remains to be demonstrated, that b must necessarily be found amongst the remainders of the series

$$r^n,\ r^{2n},\ r^{3n},\ r^{4n},\ \&\text{c.},\ r^{(x-1)n}.$$

Now, because r^m is the general root of the equation

$$x^{nw}-1=\text{M}(a),$$

we shall have

$$(r^{mn})^w-1=\text{M}(a);$$

that is, r^{mn} is a general root of the equation

$$x^w-1=\text{M}(a);$$

and since, also,

$$b^w-1=\text{M}(a),$$

it follows, that b must necessarily fall amongst one of the remainders corresponding with r^{mn}; that is, in one of the terms of the series

$$r^n,\ r^{2n},\ r^{3n},\ r^{4n},\ \&\text{c.},\ r^{(w-1)n}.$$

Remark. There is no exception to this method of solution, but it will sometimes be very laborious to find b in the above series of roots.

Ex. Required the value of x in the equation

$$x^{10}-5=\text{M}(601).$$

We have already considered this example, and have decomposed it into five equations of the second degree; we shall now attempt the solution on the principles of the last proposition.

Since $b=5$, we have, by rejecting the multiples of 601, $b^6=-1$ and $b^{12}=1$; thus $w=12$.

Now the complete solution of the equation

$$x^{120}-1=\text{M}(601),$$

found by article 201, is $x=(-140)^m$, and, consequently, x in the equation

$$x^{12}-1=\text{M}(601),$$

is $x=(-140)^{10m}=120^m$; therefore, b ought to be contained in the formula 120^m, and we find this

succeed in taking $m=5$. Therefore, the complete solution of the proposed equation is

$$x=(-140)^{5+12m}, \text{ or } x=214.(169)^m,$$

from which expression result the values

$$x=\pm 214, \ \pm 106, \ \pm 116, \ \pm 229, \ \pm 237.$$

Remark. We might have pursued this subject much farther, by finding the value of x in similar equations, in which the divisor is any power of a prime number; and, finally, for any composite number whatever: but what has been said will enable the ingenious reader to arrive at the solution of these cases, and others that may arise, by the application of the rules and principles laid down in the foregoing pages.

207. *Scholium.* In all the propositions which have been hitherto the subject of our inquiry, we have been able to pursue the investigations, and derive the results of our operations, by means of certain rules and principles, as direct and satisfactory as in any other branch of algebra; but in what follows, few or no rules can be given, and consequently much must necessarily be left to the skill and ingenuity of the analyst himself: still, however, the results that have been obtained in the preceding chapters will be found of essential service in our future inquiries, nothing more being requisite than a judicious application of them to the various cases that may occur; and it will therefore be convenient, for the sake of reference, to have exhibited here, in the form of a table, such of the foregoing resulting formulæ as are most commonly employed in Diophantine researches.

TABLE OF INDETERMINATE FORMULÆ.

FORM I.

Equation $ax - by = \pm c$.

General value of $x = mb \pm cq$,

- - - - - $y = ma \pm cp$.

In which expressions m is indeterminate, and the values of p and q result from the solution of the equation

$$ap - bq = \pm 1 \quad \text{(art. 160)}.$$

II.

Equa. $ax + by = c$.

General value of $x = cq - mb$,

- - - - - $y = ma - cp$.

Num. of solutions $= \dfrac{cq}{b} - \dfrac{cp}{a}$.

The quantities p and q being ascertained as above; also m indeterminate (art. 161).

III.

Equa. $ax + by + cz = d$.

General value of $x = (d - cz)q - mb$,

- - - - - $y = ma - (d - cz)p$.

The quantities p and q being found as above; also m indeterminate, and z any integer $< \dfrac{d}{c}$ (art. 162).

IV.

Equa. $x^2 - ay^2 = z^2$.

General value of $x = p^2 + aq^2$,

- - - - - $y = 2pq$,

- - - - - $z = p^2 - aq^2$.

In which expressions a is given, and p and q are indeterminates (art. 171).

V.

Equa. $x^2 + ay^2 = z^2$.

General value of $x = p^2 - aq^2$,

- - - - - $y = 2pq$,

- - - - - $z = p^2 + aq^2$;

a being given, and p and q being indeterminates as above (art. 171).

VI.

Equa. $ax^2 + bxy + y^2 = z^2$.

General value of $x = 2pq + bq^2$,

- - - - - $y = p^2 - aq^2$,

- - - - - $z = p^2 + bpq + aq^2$;

p and q being indeterminates, and a and b known quantities (cor. 1, art. 100).

VII.

Equa. $ax^2 + bx = z^2$.

General value of $x = \frac{bq^2}{p^2 - aq^2}$,

- - - - - $z = \frac{bpq}{p^2 - aq^2}$;

when p and q are indeterminates (art. 168).

VIII.

Equa. $m^2x^2 + bx + c = z^2$.

General value of $x = \dfrac{p^2 - cq^2}{bq^2 - 2mpq}$,

- - - - - $z = \dfrac{mp^2 + mcq^2 - bpq}{bq^2 - 2mpq}$.

Here m, b, and c, are any given numbers, and p and q indeterminates (art. 169).

IX.

Equa. $ax^2 + bx + m^2 = z^2$.

General value of $x = \dfrac{bq^2 - 2mpq}{p^2 - aq^2}$,

- - - - - $z = \dfrac{mp^2 + amq^2 - bpq}{p^2 - aq^2}$.

In which expressions a, b, and m, are known, and p and q indeterminates (art. 170).

X.

Equa. $x^2 - \text{N}y^2 = \pm 1$.

General value of $x = \dfrac{(p + q\sqrt{\text{N}})^m + (p - q\sqrt{\text{N}})^m}{2}$,

- - - - - $y = \dfrac{(p + q\sqrt{\text{N}})^m - (p - q\sqrt{\text{N}})^m}{2\sqrt{\text{N}}}$.

Where p and q are determined by the equation

$$p^2 - \text{N}q^2 = \pm 1,$$

and m is indeterminate, except that it must be even or odd, as the case may require (art. 180).

XI.

Equa. $x^2 - Ny^2 = \pm A$.

General value of $x = pm \pm Nqn$,
- - - - - $y = pn \pm qm$.

Where the values m and n are first found from the equation

$$m^2 - Nn^2 = \pm A,$$

and those of p and q from the equation (art. 181)

$$p^2 - Nq^2 = \pm 1.$$

XII.

Equa. $ax^3 + bx^2 + cx + f^2 = z^2$.

Particular value of $x = \dfrac{c^2 - 4bf^2}{4af^2}$,

or - - - - - $x = \dfrac{(8af^4 - 4bf^2c + c^3)8f^2}{(4bf^2 - c^2)^2}$.

All the coefficients, a, b, c, and f, being given and determined quantities (art. 184).

XIII.

Equa. $ax^4 + bx^3 + cx^2 + dx + f^2 = z^2$.

Particular value of $x = \dfrac{(8bf^4 - 4cdf^2 + d^3)8f^2}{16c^2f^4 - 64af^6 - 8cd^2f^2 + d^4}$.

Where a, b, c, &c., are known quantities, as above (art. 187).

XIV.

Equa. $m^2x^4+bx^3+cx^2+dx+e=z^2$.

Particular value of $x=\dfrac{16c^2m^4-64em^6-8cb^2m^2+b^4}{(8dm^4-4cbm^2+b^3)8m^2}$.

Where, also, m, b, c, d, and e, are determined quantities, as above (art. 188).

XV.

Equa. $m^2x^4+bx^3+cx^2+dx+f^2=z^2$.

Particular value of $x=\dfrac{d^2\pm 8mf^3-4cf^2}{4bf^2\mp 4mdf}$,

or - - - - - $x=\dfrac{4m^2d\pm 4mbf}{b^2\mp 8m^3f-4m^2c}$.

In these expressions m, b, c, &c., are known quantities, but, with regard to the ambiguous sign, it must be observed, that when that, in the numerator, is taken $+$, the corresponding sign, in the denominator, must be $-$; and the contrary (art. 189).

XVI.

Equa. $ax^3+bx^2+cx+f^3=z^3$.

Particular value of $x=\dfrac{(c^2-3bf^3)9f^3}{27af^6-c^3}$;

a, b, c, &c., being known quantities (art. 192).

XVII.

Equa. $m^3x^3 + bx^2 + cx + d = z^3$.

Particular value of $x = \dfrac{b^3 - 27dm^6}{(3cm^3 - b^2)9m^3}$.

Where m, b, c, &c., are given quantities, as above (art. 193).

XVIII.

Equa. $m^3x^3 + bx^2 + cx + f^3 = z^3$.

Particular value of $x = \dfrac{(c^2 - 3bf^3)9f^3}{27m^3f^6 - c^3}$,

or - - - - - - $x = \dfrac{b^3 - 27f^3m^6}{(3cm^3 - b^2)9m^3}$,

or - - - - - - $x = \dfrac{3mf^2 - c}{b - 3m^2f}$.

Where, also, m, b, c, &c., are known quantities (art. 194).

XIX.

Equa. $x^2 + axy + by^2 = z^3$.

General value of $x = t^3 - btu^2 - abu^3$,

- - - - - $y = 3t^2u + 3atu^2 + (a^2 - b)u^3$,

- - - - - $z = t^2 + atu + bu^2$.

Where a and b are known quantities, and t and u indeterminates, that may be assumed at pleasure (art. 196).

XX.

Equa. $x^2 + by^2 = z^3$.

General value of $x = t^3 - btu^2$,
- - - - - $y = t^3 - bu^3$,
- - - - - $z = t^2 + bu^2$.

Note. This is deduced from the foregoing one, by making $a = 0$.

XXI.

Equa. $x^2 + axy + by^2 = z^4$.

Gen. value of $x = t^4 - 6bt^2u^2 - 4abtu^3 - (a^2b - b^2)u^4$,

- - - $y = \begin{cases} 4t^3u + 6at^2u^2 + 4(a^2 - b)tu^3 + (a^3 \\ \quad - 2ab)u^4, \end{cases}$

- - - $z = t^2 + atu + bu^2$.

Where a and b are known quantities, and t and u indeterminates which may be assumed at pleasure (art. 197).

XXII.

Equa. $x^2 + by^2 = z^4$.

Gen. value of $x = t^4 - 6bt^2u^2 + b^2u^4$,
- - - $y = 4t^3u - 4btu^3$,
- - - $z = t^2 + bu^2$.

Note. This form is deduced from the foregoing one, by making $a = 0$.

XXIII.

Equa. $x^2 + by^2 = z^m$.

Gen. value of $x = t^m - \beta t^{m-2}u^2b + \delta t^{m-4}u^4b^2 - \&c.$,

- - - $y = \alpha t^{m-1}u - \gamma t^{m-3}u^3b + \varepsilon t^{m-5}u^5b^2 - \&c.$,

- - - $z = t^2 + bu^2$.

In which expressions b and m are known quantities, as are also 1, α, β, γ, δ, ε, &c., these letters representing the respective coefficients arising from the binomial $(t+u)^m$; but t and u are indeterminates that may be assumed at pleasure (art. 198).

XXIV.

Equa. $x^3 + cy^3 = z^2$.

General value of $x = 4t^4 - 4ctu^3$,

- - - - - $y = 8t^3u + cu^4$,

- - - - - $z = t^3 + cu^3$.

Where c is given, but t and u are indeterminates (cor., art. 199).

XXV.

Equa. $x^3 + ax^2y + bxy^2 + cy^3 = z^2$.

Particular value of $t = -\dfrac{u^2 + 2auw + (a^2 - b)w^2}{2w}$,

General value of $x = t^2 + 2cuw + acw^2$,

- - - - - $y = 2tu - 2buw - (ab - c)w^2$.

In which expressions a, b, and c, are any given quantities, u and w indeterminates; but t is limited by the above equation, and depends upon the values of u and w (art. 199).

CHAP. VI.

The Solution of Diophantine Problems.

PROB. I.

208. To divide a given square number into two other square numbers.

Let a^2 represent the given square, and x^2 and y^2 the required squares; then we have only to satisfy the equation

$$\begin{cases} a^2 = x^2 + y^2, \text{ or} \\ a^2 - y^2 = x^2. \end{cases}$$

In order to which, let us assume

$$a + y = \frac{px}{q},$$

$$a - y = \frac{qx}{p}.$$

From which we readily deduce

$$2a = \frac{px}{q} + \frac{qx}{p} = \frac{(p^2 + q^2)x}{pq},$$

$$2y = \frac{px}{q} - \frac{qx}{p} = \frac{(p^2 - q^2)x}{pq}.$$

Whence, by multiplication and division,

$$x = \frac{2pqa}{p^2 + q^2},$$

$$y = \frac{p^2 - q^2}{2pq} \times \frac{2pqa}{p^2 + q^2} = \frac{(p^2 - q^2)a}{p^2 + q^2}.$$

Where the indeterminates p and q, may be assumed at pleasure.

Cor. If a be the sum of two squares, p and q may be so assumed that $p^2+q^2=a$, or any factor of a, in which case the above expressions will be integral; and as many different integer values may be found for x and y as there are different ways of resolving a into the sum of two squares, or any of its factors.

Ex. 1. Resolve 65^2 into two other squares.

Here

$$x=\frac{(2pq\times 65)}{p^2+q^2}, \text{ and}$$

$$y=\frac{(p^2-q^2)65}{p^2+q^2}.$$

And, since $65=8^2+1^2=7^2+4^2$, we may take

$$\begin{cases} p=8 \text{ and } q=1, \text{ which gives } x=16 \text{ and } y=63; \\ p=7 \text{ and } q=4, \text{ which gives } x=56 \text{ and } y=33. \end{cases}$$

Also, since $13=3^2+2^2$ is a factor of 65, we may take

$$p=3 \text{ and } q=2, \text{ which gives } x=60 \text{ and } y=25.$$

And, again, $5=2^2+1^2$ is a factor of 65, therefore we may take

$$p=2 \text{ and } q=1, \text{ which gives } x=52 \text{ and } y=39;$$

so that

$$65^2=16^2+63^2=56^2+33^2=60^2+25^2=52^2+39^2.$$

Which are the only integral solutions that the equation admits of, but fractional answers may be obtained *ad libitum*.

PROB. II.

209. To divide a number that is equal to the sum of two given squares into two other square numbers.

Let a^2 and b^2 represent the two given squares, and x^2 and y^2 the two required ones; then we must solve the equation

$$\begin{cases} a^2+b^2=x^2+y^2, \text{ or} \\ a^2-x^2=y^2-b^2. \end{cases}$$

For which purpose let us assume

$$a+x=\frac{p(y+b)}{q},$$

$$a-x=\frac{q(y-b)}{p}.$$

Whence,

$$\begin{cases} aq+qx=py+pb, \\ ap-px=qy-qb. \end{cases}$$

Or,

$$\begin{cases} qx-py=pb-aq, \\ px+qy=qb+ap. \end{cases}$$

Now, multiplying these equations by p and q, so as to eliminate x and y, we have, by the common rules,

$$\begin{cases} pqx-p^2y=p(pb-aq), \\ pqx+q^2y=q(qb+ap). \end{cases}$$

Whence,

$$y=\frac{bq^2+2apq-bp^2}{p^2+q^2},$$

and, in the same manner,

$$x=\frac{ap^2+2bpq-aq^2}{p^2+q^2}.$$

In which expressions p and q are indeterminates, and may be assumed at pleasure.

Cor. If the given sum a^2+b^2 be such as to admit of a resolution into two other integral squares, it will be better to resolve the given number, or sum, into its factors, which, in that case, will also be

the sums of two squares, then their product will give the required squares: thus, if

$$a^2+b^2=(m^2+n^2)(m'^2+n'^2),$$

then, by art. 91,

$$a^2+b^2=(mm'\pm nn')^2+(mn'\mp m'n)^2;$$

therefore,

$$\begin{cases} x=mm'\pm nn', \\ y=mn'\mp m'n. \end{cases}$$

Ex. 1. It is required to resolve

$$85=9^2+2^2$$

into two other integral squares.

Here

$$85=5\times 17=(2^2+1^2)\times(4^2+1^2);$$

whence $m=2$ $n=1$, also $m'=4$ and $n'=1$.

Whence,

$$\begin{cases} x=2.4\pm 1. \quad =9, \text{ or } 7; \\ y=2.1\mp 4.1=2, \text{ or } 6; \end{cases}$$

that is,

$$85=9^2+2^2=7^2+6^2.$$

But, if the given number be not resolvible into factors of the form we have supposed, then it is in vain to seek for integral solutions, and we must then proceed according to the foregoing proposition.

Ex. 2. It is required to resolve

$$5=2^2+1^2$$

into two other squares.

Here $a=2$ and $b=1$; and, by taking $p=2$ and $q=3$, we have $x=\frac{29}{13}$ and $y=\frac{2}{13}$.

PROB. III.

210. To find three square numbers in arithmetical progression.

Let x^2, y^2, and z^2, represent the three required squares; and it will then be necessary to solve the equation

$$x^2+z^2=2y^2.$$

In order to which, let $x=m+n$, and $z=m-n$; then

$$x^2+y^2=2m^2+2n^2=2y^2.$$

And it only remains to find

$$m^2+n^2=y^2.$$

We have, therefore, by form v.,

$$\begin{cases} m=p^2-q^2, \\ n=2pq. \end{cases}$$

Which values, being substituted for m and n in the equations $x=m+n$, and $y=m-n$, give

$$\begin{cases} x=p^2-q^2+2pq, \\ z=p^2-q^2-2pq, \\ y=p^2+q^2. \end{cases}$$

In which formulæ p and q may be assumed at pleasure.

If, for example, we take $p=2$ $q=1$, the three squares will be 7^2, 5^2, and 1^2.

Again, assuming $p=3$ and $q=2$, we have 17^2, 13^2, 7^2, for the required squares.

2d Method. The equation

$$x^2+z^2=2y^2$$

may be put under the form

$$2y^2-x^2=z^2;$$

and this again (by art. 97) may be represented by

$$(2y+x)^2-2(y+x)^2=z^2.$$

Therefore, by form v., make

$$\begin{cases} 2y + x = p^2 + 2q^2; \\ y + x = 2pq. \end{cases}$$

Whence, by subtraction,

$$\begin{cases} y = p^2 + 2q^2 - 2pq; \\ x = 4pq - p^2 - 2q^2, \\ z = p^2 + 2q^2. \end{cases}$$

These results are apparently different from the former, but they are readily reducible to the same, and will, in their present form, equally answer the required conditions.

Ex. Assuming $p = 3$ and $q = 1$, we have $y = 5$, $x = 1$, and $z = 7$; which is the same as one of the preceding solutions.

PROB. IV.

211. To divide the sum of three square numbers, in arithmetical progression, into three other squares, which shall also be in arithmetical progression.

Let $s = a^2 + b^2 + c^2$ represent the sum of three square numbers in arithmetical progression, and let x^2, y^2, z^2, be the required squares, then it will be necessary to solve the equations

$$\begin{cases} x^2 + y^2 + z^2 = s, \\ x^2 + z^2 \qquad = 2y^2. \end{cases}$$

And here we soon see that $y^2 = \frac{1}{3}s$, and also $b = \frac{1}{3}s$, therefore $y^2 = b^2$; substituting this value of y^2, the equation is reduced to that of finding the values of x and z in the equation

$$x^2 + z^2 = 2b^2,$$

the solution of which has been given at problem ii., where we find (by making $a=b$), in that article,

$$x=\frac{bp^2+2bpq-bq^2}{p^2+q^2}=\frac{(p^2+2pq-q^2)b}{p^2+q^2},$$

$$y=\frac{bq^2+2bpq-bp^2}{p^2+q^2}=\frac{(q^2+2pq-p^2)b}{p^2+q^2}.$$

In which expressions p and q may be assumed at pleasure; and thus any number of sets of squares may be obtained, which shall be in arithmetical progression, and their sum equal to the given sum.

Ex. 1. Find three square numbers in arithmetical progression, whose sum shall be equal to

$$1^2+5^2+7^2=75.$$

Here, since $b=5$, we shall have, by assuming successively

$p=3$ $q=2$, for the squares $(\frac{85}{13})^2+5^2+(\frac{35}{13})^2=75;$

$p=4$ $q=3$, - - - - $(\frac{31}{5})^2+5^2+(\frac{17}{5})^2=75;$

$p=5$ $q=4$, - - - - $(\frac{245}{41})^2+5^2+(\frac{155}{41})^2=75;$

&c. &c. &c.

Cor. If it had been required to find three integral square numbers in arithmetical progression, that should be resolvible into other integral squares having the same property, then b must be so assumed that b^2 may be resolved into two integral squares, which may be done by making b equal to the product of any number of prime factors, each of the form $4n+1$, these having the property of being equal to the sum of two squares (cor. 2, art. 111),

and consequently their product is so likewise (art. 91); thus, if $b=5\times 13=65$, then we have the following sets of squares:

$$13^2+65^2+91^2=12675,$$
$$23^2+65^2+89^2=12675,$$
$$35^2+65^2+85^2=12675,$$
$$47^2+65^2+79^2=12675;$$

these numbers being found by the foregoing formulæ, by assuming for p and q, so that p^2+q^2 may be a divisor of 65, as in prob. i.

PROB. V.

212. To find a number such, that two given squares being each subtracted from it, the two remainders may also be squares.

Theorem. Let a^2 and b^2 be the two given squares, and resolve $\frac{a+b}{2}$ into any two unequal factors, m and m', and $\frac{a-b}{2}$ into any two unequal factors n and n', then will

$$(m^2+n^2)(m'^2+n'^2)$$

be the number required.

Demonstration. For, by art. 91,

$$(m^2+n^2)(m'^2+n'^2)=\begin{cases}(mm'+nn')^2+(mn'-m'n)^2,\\(mm'-nn')^2+(mn'+m'n)^2.\end{cases}$$

And since $\frac{a+b}{2}=mm'$, and $\frac{a-b}{2}=nn'$, therefore

$$a=mm'+nn',\ \text{and}\ b=mm'-nn';$$

and, consequently, the square of each being taken from the above product, will leave a square remainder.

Cor. Hence, when the two given squares are both even, or both odd, the question will admit of one or more solutions in whole numbers, according to the number of different ways in which $\frac{a+b}{2}$, and $\frac{a-b}{2}$, may be resolved into unequal factors.

Suppose, for example, 18^2 and 2^2 were the two given squares; here

$$\frac{18+2}{2}=2\times 5, \text{ or } 1\times 10; \text{ and}$$
$$\frac{18-2}{2}=2\times 4, \text{ or } 1\times 8.$$

Then the number of solutions will be four, which are as follows; *viz.*

$$(2^2+2^2)\times(\ 5^2+4^2)=328,$$
$$(2^2+1^2)\times(\ 5^2+8^2)=445,$$
$$(1^2+2^2)\times(10^2+4^2)=580,$$
$$(1^2+1^2)\times(10^2+8)\ =328.$$

Two of which values of the required quantities are equal, because the first factors of m and n are equal.

So that, in fact, we have only three solutions; namely,

$$\begin{cases} 328-2^2=18^2,\ 328-18^2=2^2, \\ 445-2^2=21^2,\ 445-18^2=11^2, \\ 580-2^2=24^2,\ 580-18^2=16^2. \end{cases}$$

But fractional solutions may be found *ad libitum.*

PROB. VI.

213. To find two integral numbers such that, unity being added to each, as also to their sum

and difference, the four results shall be complete squares.

Let x and y represent the required numbers, it is required to find

$$\begin{cases} x+1 \quad\quad = m^2, \\ y+1 \quad\quad = n^2, \\ x+y+1 = r^2, \\ x-y+1 = s^2. \end{cases}$$

Now here it is obvious, that the three squares r^2, m^2, and p^2, are in arithmetical progression, their common difference being y.

Let us, therefore, represent these three squares, according to prob. iii., by

$$\begin{cases} s^2 = (4pq - p^2 - 2q^2)^2, \\ m^2 = (p^2 + 2q^2 - 2pq)^2, \\ r^2 = (p^2 + 2q^2)^2. \end{cases}$$

Then we have, for their common difference,

$$y = 4p^3q - 12p^2q^2 + 8pq^3;$$

and all that is required is to find this quantity, *plus* 1, a square, or

$$4p^3q - 12p^2q^2 + 8pq^3 + 1 = n^2.$$

Assume, therefore,

$$n = 1 + 4pq^3;$$

then we have, by squaring and cancelling the like parts,

$$4p^3q - 12p^2q^2 = 16p^2q^6.$$

Whence,

$$p = 4q^5 + 3q;$$

in which expression q may be assumed at pleasure.

And thus the general values of x and y will be determined; *viz.* by first making $p = 4q^5 + 3q$, and then

$$\begin{cases} x=(p^2+2q^2-2pq)^2-1, \\ y=(1+4pq^3)^2-1. \end{cases}$$

By taking $q=1$ we have $p=7$, whence $x=1368$ and $y=840$; which numbers answer the required conditions: for

$$\begin{cases} 1368+1 = 37^2, \\ 840+1 = 29^2, \\ 1368+840+1=47^2, \\ 1368-840+1=23^2. \end{cases}$$

PROB. VII.

214. To find three or more numbers, such that the sum of their cubes may be a square, and if from this sum the square of each of the quantities be subtracted, the remainders shall be squares.

Let x, y, and z, represent the three numbers, then the conditions required are as follows; *viz.*

$$x^3+y^3+z^3=\phi^2;$$

$$\left.\begin{array}{l} \phi^2-x^2=r^2, \\ \phi^2-y^2=s^2, \\ \phi^2-z^2=t^2; \end{array}\right\} \text{ or } \left\{\begin{array}{l} \phi^2=r^2+x^2, \\ \phi^2=s^2+y^2, \\ \phi^2=t^2+z^2; \end{array}\right.$$

&c. &c. &c. &c.

Which, in their present form, appear to involve considerable difficulty; they are, however, rendered very simple, as follows:

Assume any square number, A^2, and, by problem i., resolve into two square numbers, as many ways as the problem requires; thus,

$$A^2=a^2+b^2,$$
$$A^2=a'^2+b'^2,$$
$$A^2=a''^2+b''^2.$$

&c. &c.

In which equations all the quantities that enter

are known; but these expressions will obtain also, if we introduce any indeterminate square m^2: thus,

$$\frac{A^2}{m^2}=\frac{a^2}{m^2}+\frac{b^2}{m^2},$$

$$\frac{A^2}{m^2}=\frac{a'^2}{m^2}+\frac{b'^2}{m^2},$$

$$\frac{A^2}{m^2}=\frac{a''^2}{m^2}+\frac{b''^2}{m^2}.$$

&c. &c.

And these will evidently answer the required conditions, if we make

$$\frac{b^2}{m^2}=x^2,\ \frac{b'^2}{m^2}=y^2,\ \frac{b''^2}{m^2}=z^2;$$

providing m be so assumed that

$$\frac{A^2}{m^2}=\frac{b^3}{m^3}+\frac{b'^3}{m^3}+\frac{b''^3}{m^3}+\&c.,$$

which gives

$$m=\frac{b^3+b'^3+b''^3+\&c.}{A^2}.$$

And thus we have immediately the solution of the problem proposed.

Ex. Assume $A=65$, then, by problem i., we have

$$65^2=63^2+16^2,$$
$$65^2=56^2+33^2,$$
$$65^2=60^2+25^2,$$
$$65^2=52^2+39^2.$$

Whence, $b=16$, $b'=33$, $b''=25$, $b'''=39$; and

$$m=\frac{16^3+33^3+25^3+39^3}{65^2}=\frac{114977}{4225}.$$

And, therefore, from the foregoing formulæ,

$$x=\frac{16\times 4225}{114977}=\frac{67600}{114977},$$

$$y=\frac{33\times 4225}{114977}=\frac{139425}{114977},$$

$$z=\frac{25\times 4225}{114977}=\frac{105625}{114977},$$

$$w=\frac{39\times 4225}{114977}=\frac{164775}{114977}.$$

Which are four numbers, such that the sum of their cubes is a square; and if from that sum the square of each be subtracted, the four remainders are squares.

Remark. This solution deserves particular attention, as it would be perhaps difficult to solve the problem in any other way; it is also applicable to various other questions of this kind.

PROB. VIII.

215. To find three integral square numbers, such that the sum of each two, with double the other square, may form three perfect squares.

Let x^2, y^2, and z^2, represent the required squares, and we have to find

$$\begin{cases} x^2+y^2+2z^2=r^2, \\ x^2+z^2+2y^2=s^2, \\ y^2+z^2+2x^2=t^2. \end{cases}$$

Since these quantities are all integers, it is evident that we may suppose them prime to each other; they must also be all odd numbers, as will appear by considering the possible form of squares to modulus 4.

Let then, $y=x+2p$, and $z=x+2q$, and we shall have, from the first two formulæ,

$$x^2+y^2+2z^2=4x^2+4(p+2q)x+4(p^2+2q^2),$$
$$x^2+z^2+2y^2=4x^2+4(2p+q)x+4(2p^2+q^2).$$

And, by making this first quantity equal to $4(x+f)^2$, we obtain

$$x=\frac{p^2+2q^2-f^2}{2f-p-2q}.$$

And, in the same manner, the second formula, by making it $=4(x+g)^2$, gives

$$x=\frac{2p^2+q^2-g^2}{2g-2p-q},$$

which expression must be equal; make, therefore,

$$\begin{cases} p^2+2q^2-f^2=2p^2+q^2-g^2, \\ 2f-p-2q \quad =2g-2p-q, \end{cases}$$

from which equations we readily deduce the following general values of f and g; *viz.*

$$f=\tfrac{1}{4}(5q+3p),$$
$$g=\tfrac{1}{4}(5p+3q).$$

And by substituting these values for f or g, in the above expressions, for x, we obtain

$$x=\frac{7p^2-30pq+7q^2}{8(p+q)}.$$

This value of x will satisfy the first two conditions, and we shall have, by means of this, the corresponding values of y and z, because

$$y=x+2p, \text{ and } z=x+2q;$$

so that, by multiplying each of these quantities by the common divisor $8(p+q)$, we have

$$x=\ \ 7p^2-30pq+\ \ 7q^2,$$
$$y=23p^2-14pq+\ \ 7q^2,$$
$$z=\ \ 7p^2-14pq+23q^2.$$

And with these expressions, in which p and q are indeterminates, it remains for us to fulfil the third condition,

$$y^2+z^2+2x^2=t^2.$$

Now, in order to simplify, make $p=q+\phi q$, and we have

$$x=(7\phi^2-16\phi-16)q^2,$$
$$y=(23\phi^2+32\phi+16)q^2,$$
$$z=(7\phi^2+16)q^2.$$

And these expressions being squared, and substituted for x^2, y^2, and z^2, the equation becomes, when divided by q^4,

$$\frac{169}{256}\phi^4+\phi^3+2\phi^2+2\phi+1=t^2.$$

Now this equation agrees with our form xv., preceding chapter, whence

$$\phi=\frac{4m^2d\pm 4mbf}{b^2\mp 8m^3f-4m^2c};$$

where $m=\frac{13}{16}$, $b=1$, $c=2$, $d=2$, and $f=1$; therefore, $\phi=208$, and since q may be taken at pleasure, let $q=1$, whence $p=209$; so that the required values of x, y, and z, are

$$x=18719,\ y=62609,\ z=18929;$$

and it is obvious how other answers might be obtained by changing the value of q, as well as by means of the other formulæ in form xv.

PROB. IX.

216. To find three such square numbers, that each being subtracted from the sum of the other two, the three remainders may be squares.

Let x^2, y^2, and z^2, be the required squares; it is required to find

$$\begin{cases} x^2+y^2-z^2=r^2, \\ x^2+z^2-y^2=s^2, \\ y^2+z^2-x^2=t^2. \end{cases}$$

First, by assuming

$$x=p^2+q^2,$$
$$y=p^2+pq-q^2,$$
$$z=p^2-pq-q^2,$$

we shall have

$$x^2+y^2-z^2=(p^2-q^2+2pq)^2,$$
$$x^2+z^2-y^2=(p^2-q^2-2pq)^2.$$

So that the first two conditions are fulfilled, and it only remains to make a square of our third equation, which becomes, by substituting for x, y, and z, as above,

$$y^2+z^2-x^2=p^4-4p^2q^2+q^4=t^2.$$

Now in order to reduce this to our form xv., make $p=(2+\phi)q$, which, being substituted for p in the above equation, we have

$$y^2+z^2-x^2=q^4(\phi^4+8\phi^3+20\phi^2+16\phi+1).$$

Whence, again, from form xv.,

$$\phi=\frac{d^2\pm 8mf^3-4cf^2}{4bf^2\mp 4mdf}=\frac{-23}{4};$$

because $m=1$, $b=8$, $c=20$, $d=16$, and $f=1$.

But $p=(2+\phi)q$, or $p=\frac{-15}{4}q$; therefore, $p=15$ and $q=-4$: whence

$$x=p^2+q^2 \quad\quad =241,$$
$$y=p^2+pq-q^2=149,$$
$$z=p^2-pq-q^2=269.$$

Which numbers answer the required conditions, and others might be found, by the other formulæ given at form xv., as also by changing the value of q*.

Practical Diophantine Problems.

1. To find $a+x$ and $a-x$ both squares, and to point out the limits of possibility with regard to the form of a.

Ans. $a = t^2 + u^2$.

2. To find $x^3 + y^3 + z^3 = \phi^3$ a cube.

Ans. $3^3 + 4^3 + 5^3 = 6^3$.

3. To find two numbers whose sum is a square, and also such, that each being added to the square of the other shall be a square.

Ans. Any two numbers whose sum is $\frac{1}{4}$.

4. To find three numbers in arithmetical progression, the sum of every two of which shall be a square.

Ans. $120\frac{1}{2}$, $840\frac{1}{2}$, $1560\frac{1}{2}$.

5. To find three numbers such, that the product of every two, *plus* the sum of the same two, may be a square.

Ans. 4, 9, 28.

* It was intended to have added here the solution of several other Diophantine problems, but this work having already exceeded the limits which the author had prescribed to himself, he is under the necessity of cancelling the solutions of several questions, and placing them among the following practical examples.

6. To find three such numbers, that each being added to their product shall be a square.

Ans. $\frac{1}{9}, \frac{9}{9}, \frac{40}{9}$.

7. To find two numbers, whose difference is equal to the difference of their squares, and the sum of their squares a square.

Ans. $\frac{4}{7}, \frac{3}{7}$, or any two fractions the sum of which is unity.

8. To find two such numbers, that their product, added to the sum of their squares, may be a square.

Ans. 5 and 3.

9. To find three rational right angled triangles having equal areas.

Ans.

Hyp.	*Base.*	*Perp.*
58	40	42
74	24	70
113	15	112.

10. To find three squares, whose sum is also a square.

Ans. $9, 16, \frac{144}{25}$.

11. To find a quadrangle inscribed in a circle, of which the sides and area are rational.

Ans. Sides 80, 45, 100, 63.

12. To find an oblique angled triangle such, that its three sides, perpendicular, and a line bisecting the greatest angle, may be all rational numbers.

Ans. The sides are 875, 870, 145.

13. To find a triangle such, that its three sides, perpendicular, and the line drawn from one of the angles bisecting the base, may be all expressed in rational numbers.

Ans. 480, 299, 209.

14. To find two triangular numbers such, that their sum and difference shall be both triangular numbers.

15. To find two such squares, that their product added to the square of each shall be a square.

16. To find three square numbers in harmonical proportion.

17. To find three numbers in arithmetical progression such, that the sum of their cubes may be a cube.

18. To find three numbers such, that their sum may be a square, and the sum of their squares a fourth power.

19. To find a cube number, which, added to the sum of its divisors, shall be a square.

20. To find a square such, that the sum of its divisors being subtracted from it the remainder shall be a cube.

21. To find a square such, that the sum of its divisors being subtracted from it the remainder shall be a square.

22. To find a square such, that being added to the sum of its divisors the sum shall be a square.

23. To find two squares such, that each added to the sum of its divisors shall give the same number.

24. To find two square numbers such, that one of them, and its divisors, shall be equal to the divisors of the other.

CHAP. VII.

On the Solution of the Equation $x^n - 1 = 0$, n being a Prime Number; with its Application to the Analytical and Geometrical Division of the Circle.

PROP. I.

217. All the imaginary roots of the equation

$$x^n - 1 = 0$$

are contained in the general formula

$$x^2 - 2 \cos. \frac{2k\pi}{n} + 1 = 0,$$

k being any integer not divisible by n, and π representing the semicircumference.

It is a known trigonometrical property, that if

$$2 \cos. y = x + \frac{1}{x}, \; 2 \cos. ny = x^n + \frac{1}{x^n},$$

from which two equations, *viz.*

$$2 \cos. \;\; y = x + \frac{1}{x},$$

$$2 \cos. ny = x^n + \frac{1}{x^n},$$

are readily deduced the two following,

$$x^2 \;\; - 2 \cos. \;\; y . x \;\; + 1 = 0,$$
$$x^{2n} - 2 \cos. ny . x^n + 1 = 0,$$

which must necessarily have one common root, being both derived from the same value of x; and

since these are both reciprocal equations, if x be one root, $\frac{1}{x}$ will be another: they have therefore two common roots; that is, the two roots of the first equation are also roots of the second; and, consequently, from the known theory of equations, the former is a divisor of the latter.

If, now, we make $y=\frac{2k\pi}{n}$, or $ny=2k\pi$, these equations become

$$x^2-2\cos.\frac{2k\pi}{n}x+1=0,$$

$$x^{2n}-2\cos.2k\pi x^n+1=0.$$

But the $\cos. 2k\pi=1$, 2π representing the whole circumference; therefore, the latter equation now reduces to

$$x^{2n}-2x^n+1=0, \text{ or } (x^n-1)^2=0,$$

having still for its divisor the other formula

$$x^2-2\cos.\frac{2k\pi}{n}x+1=0;$$

that is, the roots of the equation

$$(x^n-1)^2=0, \text{ or } x^n-1=0,$$

are all contained in the formula

$$x^2-2\cos.\frac{2k\pi}{n}x+1=0;$$

and, therefore, by giving to k the successive values $k=1, 2, 3, \frac{1}{2}(n-1)$, the following formulæ will be obtained; *viz.*

$$x^2-2\cos.\frac{2\pi}{n}x+1=0,$$

$$x^2-2\cos.\frac{4\pi}{n}x+1=0,$$

$$x^2 - 2\cos.\frac{6\pi}{n}x + 1 = 0,$$
$$\vdots$$
$$x^2 - 2\cos.\frac{(n-1)\pi}{n}x + 1 = 0;$$

which contain among them all the $n-1$ imaginary roots of the equation

$$x^n - 1 = 0.$$

Cor. 1. If instead of making $y = \frac{2k\pi}{n}$, we had assumed $ny = 2k\pi + \pi$, our second formula,

$$x^{2n} - 2\cos.ny.x^n + 1 = 0,$$

would have been reduced to

$$x^{2n} + 2x^n + 1 = 0, \text{ or } (x^n + 1)^2 = 0,$$

(because $\cos.(2k\pi + \pi) = -1$), having for its general factor the formula

$$x^2 - 2\cos.\frac{(2k+1)\pi}{n}x + 1 = 0,$$

which is the other branch of the *Cotesian theorem.*

Cor. 2. From the theory of equations it follows, that $2\cos.\frac{2\pi}{n}$ is equal to the sum of the two roots of the equation

$$x^2 - 2\cos.\frac{2\pi}{n}x + 1 = 0,$$

which are also two of the roots of the proposed equation, and it is obviously the same with all the other formulæ; and hence it is manifest, that the

division of the circle depends upon the solution of the equation

$$x^n - 1 = 0,$$

and, conversely, by knowing the value of $2 \cos. \frac{2\pi}{n}$, the roots of the proposed equation may be determined by the solution of a quadratic.

PROP. II.

218. All the imaginary roots of the equation

$$x^n - 1 = 0,$$

n being a prime number, are different powers of the same imaginary quantity, and all different from each other.

Before demonstrating this property of the roots of the proposed equation, it will be proper to show that, when n is a prime number, the roots of this equation cannot be the roots of any other equation

$$x^m - 1 = 0,$$

m being supposed prime to n. For, if this be possible, let R represent the common root, so that

$$R^n = 1 \text{ and } R^m = 1;$$

then, also,

$$R^{an} = 1 \text{ and } R^{bm} = 1,$$

whatever integral values are given to a and b; and, therefore, $R^{an} = R^{bm}$, or, dividing by R^{bm}, we have $R^{an-bm} = 1$; but since a and b are here indeterminates, and n and m prime to each other, such values of a and b may be found, that will make $an - bm = 1$; whence, also, $R = 1$, consequently these

equations can have no other common root besides unity.

This being premised, it will be readily shown, that all the imaginary roots of the equation

$$x^n - 1 = 0,$$

n being a prime number, are powers of the same quantity, and different from each other. For let R represent any one of these imaginary roots, then, since $R^n = 1$, so likewise $R^{2n} = 1$, $R^{3n} = 1$, $R^{4n} = 1$, &c. Therefore, if R be one root, so likewise is every term in the series

$$R,\ R^2,\ R^3,\ R^4,\ \&c.,\ R^{n-1}:$$

for each of these quantities, raised to the *nth* power, is equal to unity, which is the condition of the equation.

And, in the same manner, it may be demonstrated, that, if R^a be one imaginary root, so also is every term in the series

$$R^a,\ R^{2a},\ R^{3a},\ R^{4a},\ \&c.,\ R^{(n-1)a};$$

which roots are all different from each other. For if any two of them be equal, let them be represented by R^{pa}, and R^{qa}, or $R^{pa} = R^{qa}$, where p and q are each $< n$. And, since p and q are not equal, let $p > q$; then, dividing by R^{qa}, we have $R^{(p-q)a} = 1$; but since a is prime to n, and $p - q < n$, their product, $(p-q)a$, is also prime to n; and, therefore,

$$R^{(p-q)a} = 1$$

is impossible; for otherwise R^a would be a root of this last equation, and also a root of the equation $R^n = 1$, which we have shown to be impossible in the former part of the proposition, because $(p-q)a$

and n are prime to one another: therefore the foregoing series of roots, which belong to the equation

$$x^n - 1 = 0,$$

are different powers of the same imaginary quantity, and all different from each other.

Cor. Since $R^n = 1$, it is obvious, that $R^{n+1} = R$; $R^{n+2} = R^2$, and, universally, $R^{pa+q} = R^q$; whence it follows, that these roots may be more generally represented by the series

$$R,\ R^{an+2},\ R^{a'n+3},\ R^{a''n+4},\ \&c.$$

If, therefore, g be such a number, that its successive powers,

$$g,\ g^2,\ g^3,\ g^4,\ \&c.,\ g^{n-1},$$

when divided by n, leave different remainders, the same roots may be otherwise represented by

$$R^g,\ R^{g^2},\ R^{g^3},\ R^{g^4},\ \&c.,\ R^{g^{n-1}};$$

under which latter form it will be convenient for us to consider them in the following proposition, because this latter series will have the property of returning upon itself, if it be produced beyond the term $R^{g^{n-1}}$; for $g^{n-1} - 1$ is divisible by n (art. 87), or

$$g^{n-1} = an + 1,$$

therefore, $g^n = a'n + g$; and, consequently,

$$R^g = R^{g^n} = R^{an+g};$$

hence it is manifest, that in this series of roots it is indifferent which of them is considered as the first.

But if R be one root R^a will be another, pro-

viding a be not equal to 0, nor to n, nor to any multiple of n: therefore the same roots may be represented by

$$R^{ag},\ R^{ag^2},\ R^{ag^3},\ R^{ag^4},\ \&c.,\ R^{ag^{n-1}};$$

or by

$$R^{a},\ R^{ag},\ R^{ag^2},\ R^{ag^3},\ \&c.,\ R^{ag^{n-2}};$$

because $g^{n-1} = na + 1$, or $R^{g^{n-1}} = R$, and $R^{ag^{n-1}} = R^{a}$ &c.

The above periods of roots have, as we have seen, the property of returning upon themselves, if produced; and, since n is a prime number, $n-1$ is a composite number; making therefore $n-1 = mk$, these periods of $n-1$, or mk terms, may be decomposed into k periods of m terms each, which shall have the same property; *viz.* by being produced, the same roots will recur in the same order as at first, as appears from the following proposition.

PROP. III.

219. To decompose the $n-1$ imaginary roots of the equation

$$x^n - 1 = 0,$$

into k periods of m terms such, that each, by being produced, shall recur in the same order as at first, m and k being supposed the factors of $n-1$, or

$$n - 1 = mk.$$

The whole period of roots being

$$R,\ R^{g},\ R^{g^2},\ R^{g^3},\ R^{g^4},\ ---\ R^{g^{m(k-1)}},$$

the decomposition will stand thus:

1st period, R, $R^{g^{k}}$, $R^{g^{2k}}$, $R^{g^{3k}}$, $R^{g^{(m-1)k}}$;

2d period, R^{g}, $R^{g^{k+1}}$, $R^{g^{2k+1}}$, $R^{g^{3k+1}}$, $R^{g^{(m-1)k+1}}$;

3d period, R^{g^2}, $R^{g^{k+2}}$, $R^{g^{2k+2}}$, $R^{g^{3k+2}}$, $R^{g^{(m-1)k+2}}$;

.

.

.

k period, $R^{g^{k-1}}$, $R^{g^{2k-1}}$, $R^{g^{3k-1}}$, $R^{g^{4k-1}}$, $R^{g^{mk-1}}$.

Which are such, that, being produced, they will give over again the same periods of roots; for the following terms in these periods will be,

$$R^{g^{mk}} = R^{g^{n-1}} = R, \text{ because } g^{n-1} \doteqdot na + 1;$$

$$R^{g^{mk+1}} = R^{g^{n}} = R^{g}, \text{ because } g^{n} \doteqdot na' + g;$$

&c. &c. &c.;

and it is exactly the same with all the other periods. The method of separation is here extremely obvious, it being only necessary to write the first k terms of the general series, in the first vertical column, the second k terms in the next column, and so on.

Cor. 1. The foregoing period of roots may be represented more simply in the following manner; *viz.* by making $g^{k} = h$, with which substitution they become

R, R^{h}, R^{h^2}, R^{h^3}, $R^{h^{m-1}}$;

R^{g}, $R^{g^{h}}$, R^{gh^2}, R^{gh^3}, $R^{gh^{m-1}}$;

R^{g^2}, R^{g^2h}, $R^{g^2h^2}$, $R^{g^2h^3}$, $R^{g^2h^{m-1}}$;

.

.

.

R^{h-1}, $R^{h^{2-1}}$, $R^{h^{3-1}}$, $R^{h^{4-1}}$, $R^{h^{m-1}}$.

Hence again it follows, that any of these periods may be represented generally by

$$R^a,\ R^{ah},\ R^{ah^2},\ R^{ah^3},\ R^{ah^4},\ \&c.,\ R^{ah^{m-1}}.$$

Cor. 2. If the number of terms, in this series m, be a composite number, as $m=m'k'$, then may each of the above periods be decomposed into k' periods of m' terms each, as follows:

$$\begin{array}{llll} R^a, & R^{ah^{k'}}, & R^{ah^{2k'}}, & \&c.; \\ R^{ah}, & R^{ah^{k'+1}}, & R^{ah^{2k'+1}}, & \&c.; \\ R^{ah^2}, & R^{ah^{k'+2}}, & R^{ah^{2k'+2}}, & \&c.; \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ R^{ah^{k'-1}}, & R^{ah^{2k'-1}}, & R^{ah^{3k'-1}}, & \&c. \end{array}$$

Which, by making $h^{k'}=h'$, $R^a=S$, $R^{ah}=S^{a'}$, &c., becomes

$$\begin{array}{lllll} S, & S^{h'}, & S^{h'^2}, & S^{h'^3}, & \&c.; \\ S^{a'}, & S^{a'h'}, & S^{a'h'^2}, & S^{a'h'^3}, & \&c.; \\ S^{a'^2}, & S^{a'^2h'}, & S^{a'^2h'^2}, & S^{a'^2h'^3}, & \&c.; \end{array}$$

a similar result to the former: and in the same way the decomposition may be carried on till the number of terms in each period is a prime number, after which no farther decomposition can be effected; and all these periods will have the property of returning upon themselves when produced, as may be readily shown as above.

Remark. This decomposition of the imaginary roots of an equation of the form

$$x^n-1=0,$$

n being a prime number, into periods, and on which the solution of the equation depends, is, in practice, extremely simple, as will appear from the following examples; the foregoing complex appearance arising solely out of the generality that was necessary, in order to have a complete demonstration of the proposition. The only difficulty is in ascertaining the quantity g, so that it may be a primitive root of the indeterminate equation

$$x^{n-1} - 1 = \text{M}(n);$$

for which we might have given a rule, either in this place or in chapter v.; but as one, at least, of these roots is found among the first numbers, it seems equally expeditious, or more so, to find them by trying the small numbers 2, 3, &c., till we arrive at it, than by any direct general rule for that purpose: it may not, however, be amiss to observe, that, if $g^m > n$, and $g^m - 1$ be not divisible by n, m being a factor of $n-1$, then will g be a primitive root (art. 202), where, likewise, it is demonstrated, that there are always several such roots, except in the case $n = 3$, in which there is only one.

Ex. 1. It is required to decompose the four imaginary roots of the equation

$$x^5 - 1 = 0,$$

into two periods of two terms each, which, by being produced, shall recur in the same order.

Here, 2 is a primitive root of the equation

$$x^{5-1} - 1 = \text{M}(5),$$

because $2^2 - 1$ is not divisible by 5: the first period of roots is, therefore,

$$\text{R},\ \text{R}^2,\ \text{R}^4,\ \text{R}^8;\ \text{or}\ \text{R},\ \text{R}^2,\ \text{R}^4,\ \text{R}^3;$$

by rejecting the multiples of 5; and, therefore, the required periods are,

1st period, R, R^4;
2d period, R^2, R^3.

Ex. 2. Decompose the six imaginary roots of the equation

$$x^7 - 1 = 0,$$

into three periods of two terms each.

Here $6 = 2 \times 3$, and neither $3^2 - 1$, nor $3^3 - 1$, is divisible by 7, therefore 3 is a primitive root of the equation

$$x^7 - 1 = \text{M}(7),$$

and the powers of the roots of the proposed equation will be

$$1,\ 3,\ 3^2,\ 3^3,\ 3^4,\ 3^5;$$

or, rejecting the multiples of 7, the roots are

$$\text{R},\ \text{R}^3,\ \text{R}^2,\ \text{R}^6,\ \text{R}^4,\ \text{R}^5;$$

and, therefore, the periods sought will be,

1st period, R, R^6;
2d period, R^3, R^4;
3d period, R^2, R^5.

Ex. 3. It is required to separate the twelve imaginary roots of the equation

$$x^{13} - 1 = 0,$$

into three periods of four terms each; and these again into two periods of two terms each, which shall have the property of recurring always in the same order.

Here, 2 being a primitive root of the equation,

$$x^{12} - 1 = \text{M}(13),$$

the powers of the roots of the proposed equation will be

$$1,\ 2,\ 2^2,\ 2^3,\ 2^4,\ 2^5,\ 2^6,\ 2^7,\ 2^8,\ 2^9,\ 2^{10},\ 2^{11};$$

and, therefore, rejecting all the multiples of 13, the series of roots becomes

$$R,\ R^2,\ R^4,\ R^8,\ R^3,\ R^6,\ R^{12},\ R^{11},\ R^9,\ R^5,\ R^{10},\ R^7;$$

and the first decomposition will therefore be,

1st period, $R,\ R^8,\ R^{12},\ R^5$;
2d period, $R^2,\ R^3,\ R^{11},\ R^{10}$;
3d period, $R^4,\ R^6,\ R^9,\ R^7$.

And each of these will be divided into two periods, as follows:

1st period, $\left\{\begin{matrix} R, & R^{12}, \\ R^8, & R^5; \end{matrix}\right.$ 2d period, $\left\{\begin{matrix} R^2, & R^{11}, \\ R^3, & R^{10}; \end{matrix}\right.$

3d period, $\left\{\begin{matrix} R^4, & R^9, \\ R^6, & R^7. \end{matrix}\right.$

These examples are quite sufficient for rendering the decomposition of the roots of any equation perfectly familiar.

PROP. IV.

220. The $n-1$ imaginary roots of the equation

$$x^n - 1 = 0,$$

being decomposed into periods, as in the foregoing proposition, then will the product of the sums of any two, or more, of these periods, or any powers of those sums, be equal to the sums of similar periods.

Let

$$R^a + R^{ah} + R^{ah^2} + R^{ah^3} - - - R^{ah^{m-1}},$$

$$R^b + R^{bh} + R^{bh^2} + R^{bh^3} - - - R^{bh^{m-1}},$$

represent any two periods of roots, of which the product is required, then, since we have seen that these periods being produced, give again the same roots, and in the same order, in multiplying these quantities together, we may arrange the products in the following manner; that is, by multiplying the whole of the upper series by each term in the lower one, only beginning always with that term of the upper line, that is over the term by which we multiply, and produce the series of the upper line accordingly; thus,

$$\text{R}^{a+b} + \text{R}^{ah+b} + \text{R}^{ah^2+b} + \text{R}^{ah^3+b} + \&\text{c. } \text{R}^{ah^{m-1}+b},$$

$$\text{R}^{(a+b)h} + \text{R}^{(ah+b)h} + \text{R}^{(ah^2+b)h} + \text{R}^{(ah^3+b)h} + \&\text{c. } \text{R}^{(ah^{m-1}+b)h},$$

$$\text{R}^{(a+b)h^2} + \text{R}^{(ah+b)h^2} + \text{R}^{(ah^2+b)h^2} + \text{R}^{(ah^3+b)h^2} + \&\text{c. } \text{R}^{(ah^{m-1}+b)h^2},$$

$$\cdot$$
$$\cdot$$
$$\cdot$$

$$\text{R}^{(a+b)h^{m-1}} + \text{R}^{(ah+b)h^{m-1}} + \text{R}^{(ah^2+b)h^{m-1}} + \&\text{c.}$$

And now, taking the sums of the different vertical columns, and writing a', a'', a''', a^{iv}, &c., for $a+b$, $ah+b$, ah^2+b, &c., we have

$$\text{R}^{a'} + \text{R}^{a'h} + \text{R}^{a'h^2} + \text{R}^{a'h^3} + \&\text{c. } \text{R}^{a'h^{m-1}},$$

$$\text{R}^{a''} + \text{R}^{a''h} + \text{R}^{a''h^2} + \text{R}^{a''h^3} + \&\text{c. } \text{R}^{a''h^{m-1}},$$

$$\text{R}^{a'''} + \text{R}^{a'''h} + \text{R}^{a'''h^2} + \text{R}^{a'''h^3} + \&\text{c. } \text{R}^{a'''h^{m-1}},$$

&c. &c. &c.

Each of which new periods consists of m terms, and they are similar periods to those from the multiplication of which they were produced; because, if R^a be any imaginary root of the equation

$$x^n - 1 = 0,$$

$R^{a'}$ is another, providing a' be not divisible by n; and if a' be equal to n, or to any multiple of n, then, because $R^{na'}=1$, the sum of the roots in that period will be equal to as many units as the period has terms, as is evident.

The proposition, therefore, having been demonstrated for the product of two periods, it must necessarily be true for any number of periods; and since there is nothing in the foregoing operation to prevent us from supposing a to be equal b, or, in other words, that the two periods that we have multiplied together are equal, the same is evidently true of any powers of those periods; namely, that they may always be represented by the sums of simple periods similar to themselves.

Cor. We are thus furnished with the following easy method of obtaining those products, or powers; *viz.*

Let $\int(R^a)$, $\int(R^b)$, represent the sums of any two periods, as

$$\int(R^a)=R^a+R^{a'}+R^{a''}+R^{a'''},$$
$$\int(R^b)=R^b+R^{b'}+R^{b''}+R^{b'''}.$$

Under which form we shall have

$$\int(R^a)=\int(R^{a'})=\int(R^{a''});$$

that is, the sum of the periods is the same, whichever is the leading term, because the periods are recurring ones, and the same have place with all other periods: then will

$$\int(R^a)\times\int(R^b)=\int(R^{a+b})+\int(R^{a'+b})+\int(R^{a''+b})+\&c.$$

which formula will be of particular use in the solution of the following examples, the principle of which is to subdivide the original period of roots

into two or more periods, as in the preceding proposition; then, if there are only two, the sums of these separate periods may be ascertained, by knowing the collective sum of the two, which is always given, and the product of the same two, which is obtained from the above formula; and having thus the sum of two quantities, and their product, the quantities themselves are easily found by a quadratic; if there are three periods, then, beside the sum of these three, we must know the sum of the products of every two of them, and the product of all three, whence the separate sums are found by means of a cubic equation, and so on.

221. We may now proceed to the solution of a few examples, to illustrate what has been demonstrated in the foregoing articles.

Ex. 1. Required the cos. $\frac{360^\circ}{5} = 72^\circ$, and the imaginary roots of the equation

$$x^5 - 1 = 0.$$

The imaginary roots of this equation being decomposed into two periods, by means of their powers (as in ex. 1, art. 219), and representing the sums of these periods by p, p'; that is,

$$f(\text{R}^1) = p = \text{R} + \text{R}^4,$$
$$f(\text{R}^2) = p' = \text{R}^2 + \text{R}^3:$$

it will only be necessary to find the values of p and p'; that is, the sum of the two imaginary roots $\text{R} + \text{R}^4$, or $\text{R}^2 + \text{R}^3$, which is readily obtained by means of the foregoing proposition, and the known property of equations; *viz.* that the sum of the roots of any equation is equal to the coefficient of

the second term, which, in the present case, is zero; so that

$$\begin{aligned} 1+\text{R}+\text{R}^2+\text{R}^3+\text{R}^4 &= 0, \text{ or} \\ p+p'+1 \quad - \quad &= 0, \text{ or} \\ p+p' \quad - \quad - \quad &= -1. \end{aligned}$$

Again, by cor., art. 220,

$$f(\text{R}^1)\times f(\text{R}^2)=pp'=f(\text{R}^3)+f(\text{R}^1)=p'+p;$$

therefore, $p+p'=-1$, and $pp'=-1$; and, consequently, the equation which has for its roots the quantities p, p', will be

$$p^2+p-1=0.$$

Whence we obtain

$$p=\frac{-1+\sqrt{5}}{2}, \text{ and } p'=\frac{-1-\sqrt{5}}{2};$$

which expressions represent $2\cos.\dfrac{360^\circ}{5}$, and $2\cos.\dfrac{2.360^\circ}{5}$: therefore,

$$\cos.\ 72^\circ=\frac{-1+\sqrt{5}}{4}=\cdot 3090170,$$

$$\cos.\ 144^\circ=\frac{-1-\sqrt{5}}{4}=-\cdot 8090170.$$

The first of which values alone is obviously sufficient for the division of the circle into five equal parts. And, having thus determined the values of these cosines, we have, for finding the imaginary roots of the proposed equation, the two following quadratics:

$$x^2-\left(\frac{-1+\sqrt{5}}{2}\right)x+1=0,$$

$$x^2-\left(\frac{-1-\sqrt{5}}{2}\right)x+1=0;$$

which, with the real root 1, completes the solution of the equation.

Ex. 2. Find the cosine of $\frac{360^\circ}{7}$, and the imaginary roots of the equation

$$x^7 - 1 = 0.$$

Having decomposed the powers of the imaginary roots of this equation, or, which is the same, the roots of the indeterminate equation

$$x^6 - 1 = \text{M}(7),$$

into three periods of two terms each (ex. 2, art. 219), and representing the sums of these periods by p, p', p''; that is,

$$p = \text{R} + \text{R}^6,$$
$$p' = \text{R}^3 + \text{R}^4,$$
$$p'' = \text{R}^2 + \text{R}^5;$$

the object of inquiry will be, to ascertain the values of $p + p' + p''$, of $pp' + pp'' + p'p''$, and of $pp'p''$; for then the cubic equation, having these quantities for its coefficients, will evidently have for its roots p, p', and p''.

First, then,

$$p + p' + p'' = -1,$$

from the known theory of equations, and by cor., art. 220,

$$pp' = p' + p'',$$
$$p'p'' = p'' + p,$$
$$pp'' = p' + p;$$

therefore,

$$pp' + p'p'' + pp'' = 2(p + p' + p'') = -2.$$

Again, multiplying the first of the above products by p'' gives

$$pp'p'' = p'p'' + p''p''.$$

Now

$$p'p''=p''+p;$$

and, by cor., art. 220, and

$$p''p''=p'+2;\text{ that is, }=\int(4)+\int(7),$$

the last of which, *viz.* $\int(R^7)=2$, by the same article; therefore,

$$pp'p''=p+p'+p''+2=+1.$$

Hence the cubic equation that has p, p', and p'', for its roots, is

$$p^3+p^2-2p-1=0;$$

and, therefore, conversely, the roots of this cubic will be the values p, p' and p'', whence we find

$$p = \quad 1\cdot2469796,$$
$$p' = -1\cdot8019376,$$
$$p'' = -\quad \cdot4450420.$$

And hence again,

$$\cos.\frac{360^\circ}{7}=\frac{1\cdot2469796}{2}=\cdot6234898;$$

which is sufficient for the division of the circle into seven equal parts.

And by means of the above quantities p, p', p'', we shall have the three following quadratics; *viz.*

$$x^2-p\ x+1=0,$$
$$x^2-p'\ x+1=0,$$
$$x^2-p''x+1=0,$$

which contain in them all the different imaginary roots of the proposed equation.

Ex. 3. Find the cosine of $\frac{360^\circ}{13}$, and the roots of the equation

$$x^{13}-1=0.$$

The solution of this problem will be effected by means of a cubic and two quadratics, or a cubic and one quadratic, so far as it relates to the division of the circle into thirteen equal parts; observing, that we must finish with the quadratic, in order that we may know the sum of two of its roots: the period of roots must therefore be first divided into three periods of four terms each, as in ex. 3, art. 219.

Whence,

$$p = \text{R}^1 + \text{R}^8 + \text{R}^{12} + \text{R}^5,$$
$$p' = \text{R}^2 + \text{R}^3 + \text{R}^{11} + \text{R}^{10},$$
$$p'' = \text{R}^4 + \text{R}^6 + \text{R}^9 + \text{R}^7.$$

And here, as in the foregoing example, it will be necessary to find the values of

$p + p' + p''$, of $pp' + p'p'' + pp''$, and of $pp'p''$,

in order to ascertain the cubic equation that has these quantities for its roots.

Now,

$$p + p' + p'' = -1,$$

by the theory of equations, and by cor., art. 219,

$$pp' = p' + p' + p + p'' = p + 2p' + p'',$$
$$p'p'' = p'' + p'' + p' + p = p' + 2p'' + p,$$
$$pp'' = p + p + p' + p'' = p' + 2p + p''.$$

Whence,

$$pp' + p'p'' + pp'' = 4(p + p' + p'') = -4.$$

Again,

$$pp'p'' = pp'' + 2p'p'' + p''p''.$$

But

$$pp'' = p' + 2p + p'',$$
$$2p'p'' = 2p' + 4p'' + 2p,$$
$$p''p'' = 2p' + p + 4 = \int(\text{R}^8) + 2\int(\text{R}^2) + \int(\text{R}^{13}).$$

Hence,

$$pp'p'' = 5(p + p' + p'') + 4 = -5 + 4 = -1.$$

Wherefore the cubic equation, having p, p', p'', for its roots, is

$$p^3 + p^2 - 4p + 1 = 0:$$

and hence these values become known, each of which is the sum of four roots. And now, in order to get the sum of each pair of roots, the foregoing periods must be again subdivided into periods of two, the sums of which, for distinction sake, are represented by q, q', &c., as follows; *viz.*

$$\text{Period } p, \text{ into } \begin{cases} q \;\;= R^1 + R^{12}, \\ q' \;= R^8 + R^5. \end{cases}$$

$$\text{Period } p', \text{ into } \begin{cases} q'' = R^2 + R^{11}, \\ q''' = R^3 + R^{10}. \end{cases}$$

$$\text{Period } p'', \text{ into } \begin{cases} q^{\text{iv}} = R^4 + R^9, \\ q^{\text{v}} \;= R^6 + R^7. \end{cases}$$

Now,

$$q + q' = p,$$

which is known from the preceding equation, and

$$qq' = q^{\text{iv}} + q^{\text{v}} = p'',$$

which is also known.

Whence, the equation containing the roots q, q', is determined, being

$$q^2 - pq + p'' = 0;$$

and the value of q in this will be equal to $2 \cos. \dfrac{360°}{13}$; and, by means of this, the roots of the proposed equation will be determined.

It does not appear, from what has been done, which of these periods ought to represent the

$\cos. \frac{360^\circ}{13}$; but this becomes immediately evident from considering, that the cos. of this angle will be positive, and greater than the cos. of any of the other angles,

$$\frac{2.360^\circ}{13}, \frac{3.360^\circ}{13}, \&c.;$$

and, therefore, that period q must be assumed into which p enters positively: and, in the same way, we readily discover the particular period which represents the cos. of any other angles, as, likewise, the negative from the positive, &c., by which means the apparent ambiguity is avoided.—These observations must be particularly attended to in the following example.

Ex. 4. Find the cosine of $\frac{360^\circ}{17}$, and the roots of the equation

$$x^{17} - 1 = 0.$$

Since 17 is a prime number of the form $2^m + 1$, or $17 = 2^4 + 1$, the roots of the above equation may be obtained by four quadratic equations, and the cosine of $\frac{360^\circ}{17}$ by three quadratic equations; in order to which, the imaginary roots of the equation

$$x^{17} - 1 = 0$$

must be decomposed, first, into two periods of eight terms each, then these into two periods of four, and these again into two periods of two terms each. Now 3 being a primitive root of the equation

$$x^{16} - 1 = \text{M}(17),$$

the whole period of powers will be,

$$\begin{cases} 1,\ 3,\ 3^2,\ 3^3,\ 3^4,\ 3^5,\ 3^6,\ 3^7,\ 3^8,\ 3^9,\ 3^{10},\ 3^{11},\ 3^{12}, \\ \quad 3^{13},\ 3^{14},\ 3^{15};\ \text{or} \end{cases}$$

$$\begin{cases} 1,\ 3,\ 9,\ 10,\ 13,\ 5,\ 15,\ 11,\ 16,\ 14,\ 8,\ 7,\ 4, \\ \quad 12,\ 2,\ 6; \end{cases}$$

by rejecting the multiples of 17.

Whence (by art. 219) the first two periods will be

$$p = R^1 + R^9 + R^{13} + R^{15} + R^{16} + R^8 + R^4 + R^2,$$
$$p' = R^3 + R^{10} + R^5 + R^{11} + R^{14} + R^7 + R^{12} + R^6.$$

Now

$$p + p' = -1;$$

and

$$pp' = p + p' + p + p + p + p' + p' + p' = 4(p + p') = -4.$$

Hence the quadratic equation containing the roots p, p', will be

$$p^2 + p - 4 = 0.$$

Whence,

$$p = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{17},\ \text{and}\ p' = -\tfrac{1}{2} - \tfrac{1}{2}\sqrt{17}.$$

Again, the periods of roots p, p', must be now decomposed into the four following periods, the sums of which are, for distinction sake, represented by q, q'; *viz.*

$$\text{Period } p, \begin{cases} q \ = R^1 + R^{13} + R^{16} + R^4, \\ q' \ = R^9 + R^{15} + R^8 + R^2. \end{cases}$$

$$\text{Period } p', \begin{cases} q'' = R^3 + R^5 + R^{14} + R^{12}, \\ q''' = R^{10} + R^{11} + R^7 + R^6. \end{cases}$$

And here we have

$$q + q' = p = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{17},$$
$$qq' = q''' + q'' + q' + q = p + p' = -1.$$

Whence the quadratic equation containing the roots q, q', is

$$q^2 - pq - 1 = 0:$$

consequently,

$$q = \tfrac{1}{2}p + \tfrac{1}{2}\sqrt{(4+p^2)}, \text{ and } q' = \tfrac{1}{2}p - \tfrac{1}{2}\sqrt{(4+p^2)}.$$

In the same way,

$$q'' = \tfrac{1}{2}p' + \tfrac{1}{2}\sqrt{(4+p'^2)}, \text{ and } q''' = \tfrac{1}{2}p' - \tfrac{1}{2}\sqrt{(4+p'^2)}.$$

Again, the above periods of q, q', q'', &c., are each decomposed into two periods of two terms each, which new periods are represented by t, t', t'', &c.; *viz.*

$$\text{Period } q, \text{ into } \begin{cases} t = R^1 + R^{16}, \\ t' = R^{13} + R^4. \end{cases}$$

$$\text{Period } q', \text{ into } \begin{cases} t'' = R^9 + R^8, \\ t''' = R^{15} + R^2. \end{cases}$$

$$\text{Period } q'', \text{ into } \begin{cases} t^{iv} = R^3 + R^{14}, \\ t^{v} = R^5 + R^{12}. \end{cases}$$

$$\text{Period } q''', \text{ into } \begin{cases} t^{vi} = R^{10} + R^7, \\ t^{vii} = R^{11} + R^6. \end{cases}$$

Now

$$t + t' = q = \tfrac{1}{2}p + \tfrac{1}{2}\sqrt{(4+p^2)},$$

and

$$tt' = t^{iv} + t^{v} = q'' = \tfrac{1}{2}p' + \tfrac{1}{2}\sqrt{(4+p'^2)}.$$

Therefore the quadratic equation containing the roots t, t', is

$$t^2 - qt + q'' = 0.$$

Whence,

$$\begin{cases} t = \tfrac{1}{2}q + \tfrac{1}{2}\sqrt{(q^2 - 4q'')}, \\ t' = \tfrac{1}{2}q - \tfrac{1}{2}\sqrt{(q^2 - 4q'')}. \end{cases}$$

The first of these is the greatest positive root,

and is, therefore, the value of $2\cos.\dfrac{360^\circ}{17}$; which, by substituting for q and q'', their respective values, in terms of p and p', becomes $2\cos.\dfrac{360^\circ}{17} =$

$$\left\{\begin{array}{l}\frac{1}{2}\{\frac{1}{2}p+\frac{1}{2}\sqrt{(4+p^2)}\}+\frac{1}{2}\sqrt{\{\frac{1}{2}p+\frac{1}{2}\sqrt{(4+p^2)}\}^2-}\\ \quad 4\{\frac{1}{2}p'+\frac{1}{2}\sqrt{(4+p'^2)}\}.\end{array}\right.$$

Again, reestablishing the values of p, p', we have, in numbers, $2\cos.\dfrac{360^\circ}{17} =$

$$\left\{\begin{array}{l}\frac{1}{2}\{\frac{1}{2}(-\frac{1}{2}+\frac{1}{2}\sqrt{17})+\frac{1}{2}\sqrt{\frac{1}{2}(17-\sqrt{17})}\}+\\ \quad \frac{1}{2}\sqrt{\{\frac{1}{2}(-\frac{1}{2}+\frac{1}{2}\sqrt{17})+\frac{1}{2}\sqrt{\frac{1}{2}(17-\sqrt{17})}\}^2-}\\ \quad 4\{\frac{1}{2}(-\frac{1}{2}-\frac{1}{2}\sqrt{17})+\frac{1}{2}\sqrt{\frac{1}{2}(17+\sqrt{17})}\},\end{array}\right.$$

which is the true numeral value of $2\cos.\dfrac{360^\circ}{17}$; whence it is manifest, that, by the construction of three quadratic equations, a 17 sided polygon may be inscribed *geometrically* in a circle.

We might have added here the solution of the equations,

$$x^{19}-1=0,\ x^{37}-1=0,\ x^{73}-1=0,$$

and many others; but they are left as exercises for the reader.

222. *Scholium.* From what has been demonstrated, it appears, that the equations by which the circle may be divided into a prime number of equal parts n, depend upon the factors of $n-1$; that is, upon the subdivision of its $n-1$ imaginary roots into periods; so, if $n-1=a^\alpha b^\beta c^\gamma$, then the solution will be effected by α equations of the degree a, β of the degree b, and γ of the degree c: thus, if $n=11$, then $10=2^1 5^1$; and, therefore, the solution depends upon one equation of the fifth de-

gree, and one of the second. For, in this case, we can only decompose the ten imaginary roots into five periods of two terms each, or into two periods of five terms each; and, in the first instance, it is obvious, that in order to get the sum of all the p's, as $p+p'+p''+p'''$, &c., the sum of the product of every two, of every three, &c., the equation must necessarily rise to the fifth degree. And if, according to the other division, the roots were resolved into two periods of five terms each, though the values of these periods would be found by a quadratic, yet this would be of no use, as we should thus have only the value of the sum of five of the roots, whereas it appears, from cor. 2, art. 117, that it is only by knowing the sum of two roots the solution of the equation can be determined rationally. It is necessary, therefore, in all cases, to manage the subdivisions so, that the final equation may be a quadratic; that is, so that the number of terms in each period, in the last instance, shall not exceed two; which may always be done, because n being a prime number, $n-1$ is always even; and thus, when $n-1$ is any power of 2 (as we can then at every step divide each period into two others), it follows, that the solution of such an equation may always be effected by means of quadratic equations only: and, consequently, a polygon of such a number of sides may be inscribed geometrically in a circle. Now, 5, 17, 257, 65537, are prime numbers of this form, and therefore each of these admits of a geometrical construction. We know also, from other principles, that if any two polygons of an unequal number of sides, prime to each other, can be in-

scribed geometrically in a circle, that the polygon, the number of sides of which is equal to the product of these two, can also be inscribed geometrically.

For let a and b represent the number of sides of two polygons, each inscribable in a circle, a and b being prime to each other; then it is to be demonstrated, that the polygon, the number of whose sides is equal to ab, is also inscribable. Now the angles at the centre of these polygons, will be

$$\frac{360°}{a},\ \frac{360°}{b},\ \frac{360°}{ab};$$

and if it can be shown that the difference of any multiples of the two first, can be made equal to the third, the truth of what is advanced will be evident. Let, then, $\frac{360°n}{a}$, and $\frac{360°m}{b}$, represent any multiples of the angles of the two first, then the difference will be equal to $\frac{360°(nb-ma)}{ab}$, which is to be equal to $\frac{360°}{ab}$; we have, therefore,

$$360°(nb-ma)=360°, \text{ or } nb-ma=1;$$

and, since a and b are prime to each other, such values of m and n may be found, $< a$ and b, as will answer this condition; and, consequently, the third polygon, of which the number of sides is ab, may be inscribed by means of the two first. Also all polygons, of which the number of sides is any power of 2, may be inscribed by continual bisections: and again, all those whose number of sides is equal to the product of any inscribable polygon, into any power of 2. And hence we have

the following series of polygons, each of which admits of a geometrical construction; *viz.*

Polygons of less than 100 *Sides, admitting of a Geometrical Construction.*

No. of Sides.	*No. of Sides.*	*No. of Sides.*
3 = trigon.	16 = 2^4	48 = 3.2^4
4 = 2^2	17 = 2^4+1	51 = 17.3
5 = 2^2+1	20 = 5.2^2	60 = 15.2^2
6 = 2.3	24 = 3.2^3	64 = 2^6
8 = 2^3	30 = 15.2	68 = 17.2^2
10 = 2.5	32 = 2^5	80 = 5.2^4
12 = 3.2^2	34 = 17.2	85 = 17.5
15 = 5.3	40 = 5.2^3	96 = 3.2^5

To the above, we may add the three consecutive polygons,

$$255, \ 256, \ 257,$$

each of which is inscribable in a circle; for

$$255 = 3.5.17, \ 256 = 2^8, \text{ and}$$
$$257 = 2^8 + 1, \text{ a prime.}$$

The next three consecutive polygons, that admit of a geometrical construction, are the following; *viz.*

$$65535 = 255 \times 257,$$
$$65536 = 2^{16},$$
$$65537 = 2^{16} + 1, \text{ a prime.}$$

We shall here conclude these investigations, and refer the reader, who wishes for a more general developement of the above principles, to the *Disquisitiones Arithmeticæ, by M. Gauss;* or the French translation of the same, under the title of *Recherches Arithmetiques;* or to the second edition of the *Théorie des Nombres, by M. Legendre.*

Table of Prime Numbers to 4000.

2	233	547	877	1229	1597	1993	2371	2749	3187	3581
3	239	557	881	1231	1601	1997	2377	2753	3191	3583
5	241	563	883	1237	1607	1999	2381	2767	3203	3593
7	251	569	887	1249	1609	2003	2383	2777	3209	3607
11	257	571	907	1259	1613	2011	2389	2789	3217	3613
13	263	577	911	1277	1619	2017	2393	2791	3221	3617
17	269	587	919	1279	1621	2027	2399	2797	3229	3623
19	271	593	929	1283	1627	2029	2411	2801	3251	3631
23	277	599	937	1289	1637	2039	2417	2803	3253	3637
29	281	601	941	1291	1657	2053	2423	2819	3257	3643
31	283	607	947	1297	1663	2063	2437	2833	3259	3659
37	293	613	953	1301	1667	2069	2441	2837	3271	3671
41	307	617	967	1303	1669	2081	2447	2843	3299	3673
43	311	619	971	1307	1693	2083	2459	2851	3301	3677
47	313	631	977	1319	1697	2087	2467	2857	3307	3691
53	317	641	983	1321	1699	2089	2473	2861	3313	3697
59	331	643	991	1327	1709	2099	2477	2879	3319	3701
61	337	647	997	1361	1721	2111	2503	2887	3323	3709
67	347	653	1009	1367	1723	2113	2521	2897	3329	3719
71	349	659	1013	1373	1733	2129	2531	2903	3331	3727
73	353	661	1019	1381	1741	2131	2539	2909	3343	3733
79	359	673	1021	1399	1747	2137	2543	2917	3347	3739
83	367	677	1031	1409	1753	2141	2549	2927	3359	3761
89	373	683	1033	1423	1759	2143	2551	2939	3361	3767
97	379	691	1039	1427	1777	2153	2557	2953	3371	3769
101	383	701	1049	1429	1783	2161	2579	2957	3373	3779
103	389	709	1051	1433	1787	2179	2591	2963	3389	3793
107	397	719	1061	1439	1789	2203	2593	2969	3391	3797
109	401	727	1063	1447	1801	2207	2609	2971	3407	3803
113	409	733	1069	1451	1811	2213	2617	2999	3413	3821
127	419	739	1087	1453	1823	2221	2621	3001	3433	3823
131	421	743	1091	1459	1831	2237	2633	3011	3449	3833
137	431	751	1093	1471	1847	2239	2647	3019	3457	3847
139	433	757	1097	1481	1861	2243	2657	3023	3461	3851
149	439	761	1103	1483	1867	2251	2659	3037	3463	3853
151	443	769	1109	1487	1871	2267	2663	3041	3467	3863
157	449	773	1117	1489	1873	2269	2671	3049	3469	3877
163	457	787	1123	1493	1877	2273	2677	3061	3491	3881
167	461	797	1129	1499	1879	2281	2683	3067	3499	3889
173	463	809	1151	1511	1889	2287	2687	3079	3511	3907
179	467	811	1153	1523	1901	2293	2689	3083	3517	3911
181	479	821	1163	1531	1907	2297	2693	3089	3527	3917
191	487	823	1171	1543	1913	2309	2699	3109	3529	3919
193	491	827	1181	1549	1931	2311	2707	3119	3533	3923
197	499	829	1187	1553	1933	2333	2711	3121	3539	3929
199	503	839	1193	1559	1949	2339	2713	3137	3541	3931
211	509	853	1201	1567	1951	2341	2719	3163	3547	3943
223	521	857	1213	1571	1973	2347	2729	3167	3557	3947
227	523	859	1217	1579	1979	2351	2731	3169	3559	3967
229	541	863	1223	1583	1987	2357	2741	3181	3571	3989

Table containing the least Values of p and q in the Equation $p^2 - Nq^2 = 1$, for every Value of N, from 2 to 102.

N	q	p	N	q	p
2	2	3	54	66	485
3	1	2	55	12	89
5	4	9	56	2	15
6	2	5	57	20	151
7	3	8	58	2574	19603
8	1	3	59	69	530
10	6	19	60	4	31
11	3	10	61	226153980	1766319049
12	2	7	62	8	63
13	180	649	63	1	8
14	4	15	65	16	129
15	1	4	66	8	65
17	8	33	67	5967	48842
18	4	17	68	4	33
19	39	170	69	936	7775
20	2	9	70	30	251
21	12	55	71	413	3480
22	42	197	72	2	17
23	5	24	73	267000	2281249
24	1	5	74	430	3699
26	10	51	75	3	26
27	5	26	76	6630	57799
28	24	127	77	40	351
29	1820	9801	78	6	53
30	2	11	79	9	80
31	273	1520	80	1	9
32	3	17	82	18	163
33	4	23	83	9	82
34	6	35	84	6	55
35	1	6	85	30996	285769
37	12	73	86	1122	10405
38	6	37	87	3	28
39	4	25	88	21	197
40	3	19	89	53000	500001
41	320	2049	90	2	19
42	2	13	91	165	1574
43	531	3482	92	120	1151
44	30	199	93	1260	12151
45	24	161	94	221064	2143295
46	3588	24335	95	4	39
47	7	48	96	5	49
48	1	7	97	6377352	62809633
50	14	99	98	10	99
51	7	50	99	1	10
52	90	649	101	20	201
53	9100	66249	102	10	101

FINIS.

THE FOLLOWING WORKS

OF

JOHN BONNYCASTLE, ESQ.

PROFESSOR OF MATHEMATICS AT THE ROYAL MILITARY ACADEMY, WOOLWICH.

1. AN INTRODUCTION TO ARITHMETIC; or, a complete Exercise Book, for the Use both of Teachers and Students: being the first Part of a general Course of Mathematics, with Notes, containing the Reason of every Rule, demonstrated from the most simple and evident Principles: together with some of the most useful Properties of Numbers, and such other Particulars as are calculated to elucidate the more abstruse and interesting Parts of the Science. Price 8s. boards.

2. THE SCHOLAR'S GUIDE TO ARITHMETIC; or, a complete Exercise Book, for the Use of Schools; with Notes, containing the Reason of every Rule, demonstrated from the most simple and evident Principles: together with some of the most useful Properties of Numbers, and general Theorems for the more extensive Use of the Science. Ninth edition, 1808. 12mo. 2s. 6d. bound.

3. AN INTRODUCTION TO MENSURATION AND PRACTICAL GEOMETRY: with Notes, containing the Reason of every Rule, concisely and clearly demonstrated. Tenth edition. 4s. bound.

4. AN INTRODUCTION TO ALGEBRA; with Notes and Observations; designed for the Use of Schools and Places of public Education. Eighth edition. 4s. bound.

5. AN INTRODUCTION TO ASTRONOMY; in a Series of Letters from a Preceptor to his Pupil: in which the more useful and interesting Parts of the Science are clearly and familiarly explained. Fifth edition, improved. Illustrated with Copper-plates. 9s. boards.

6. THE ELEMENTS OF GEOMETRY, or an Abridgment of the first six, and the eleventh and twelfth Books of Euclid: with Notes, Critical and Explanatory. Fifth edition. 6s. bound.

7. A TREATISE ON PLANE AND SPHERICAL TRIGONOMETRY: with their most useful Applications. 12s. boards.

Printed for J. Johnson and Co., St. Paul's Church-yard.

AN
INTRODUCTION
TO
NATURAL PHILOSOPHY.

ILLUSTRATED WITH COPPER-PLATES.

BY WILLIAM NICHOLSON.

The Fifth edition, with Improvements. 2 vols. 8vo. 16s. boards.

THE NEW
PRACTICAL NAVIGATOR;

BEING A COMPLETE

EPITOME OF NAVIGATION:

TO WHICH ARE ADDED,

All the Tables requisite for determining the Latitude and Longitude at Sea: containing the different Kinds of Sailing, and necessary Corrections for Lee-way, Variation, &c., exemplified in a Journal at Sea.

TOGETHER WITH

All necessary Instructions for determining the Latitude by DOUBLE ALTITUDES of the Sun, by the Moon, the Planets, and fixed Stars; and for ascertaining the LONGITUDE by the LUNAR OBSERVATIONS and other Methods.

The Manner of finding and knowing the Planets and fixed Stars, by Calculation and Planispheres.

The Art of Surveying Sea-coasts and Harbours.

An Abstract of Practical Seamanship, showing the Method of working a Ship in all difficult Cases at Sea.

The Manner of exercising Ship's Companies of War, describing the Exercise of the great Guns, and the requisite Manœuvres for attacking or defending a Ship.

The Method of recovering Ships in different Situations of Distress, and keeping them from a Lee-shore, with the best Means of saving Persons from Wrecks; and the Process of recovering drowned People, recommended by the Royal Humane Society; with a Variety of Articles not to be found in any other Book of this Kind.

The Whole illustrated with Engravings, and rendered easy to the most common Capacity.

The Tables in this Book have been examined by three Persons; and, it is trusted, are the most correct extant. So that this Book will be found fully sufficient either for the Teacher or for Practice at Sea.

BY JOHN HAMILTON MOORE,
Teacher of Navigation.

The Eighteenth edition; enlarged and carefully improved, by JOSEPH DESSIOU. 8vo. 12s. bound.

Printed by C. Wood,
Poppin's Court, Fleet Street, London.